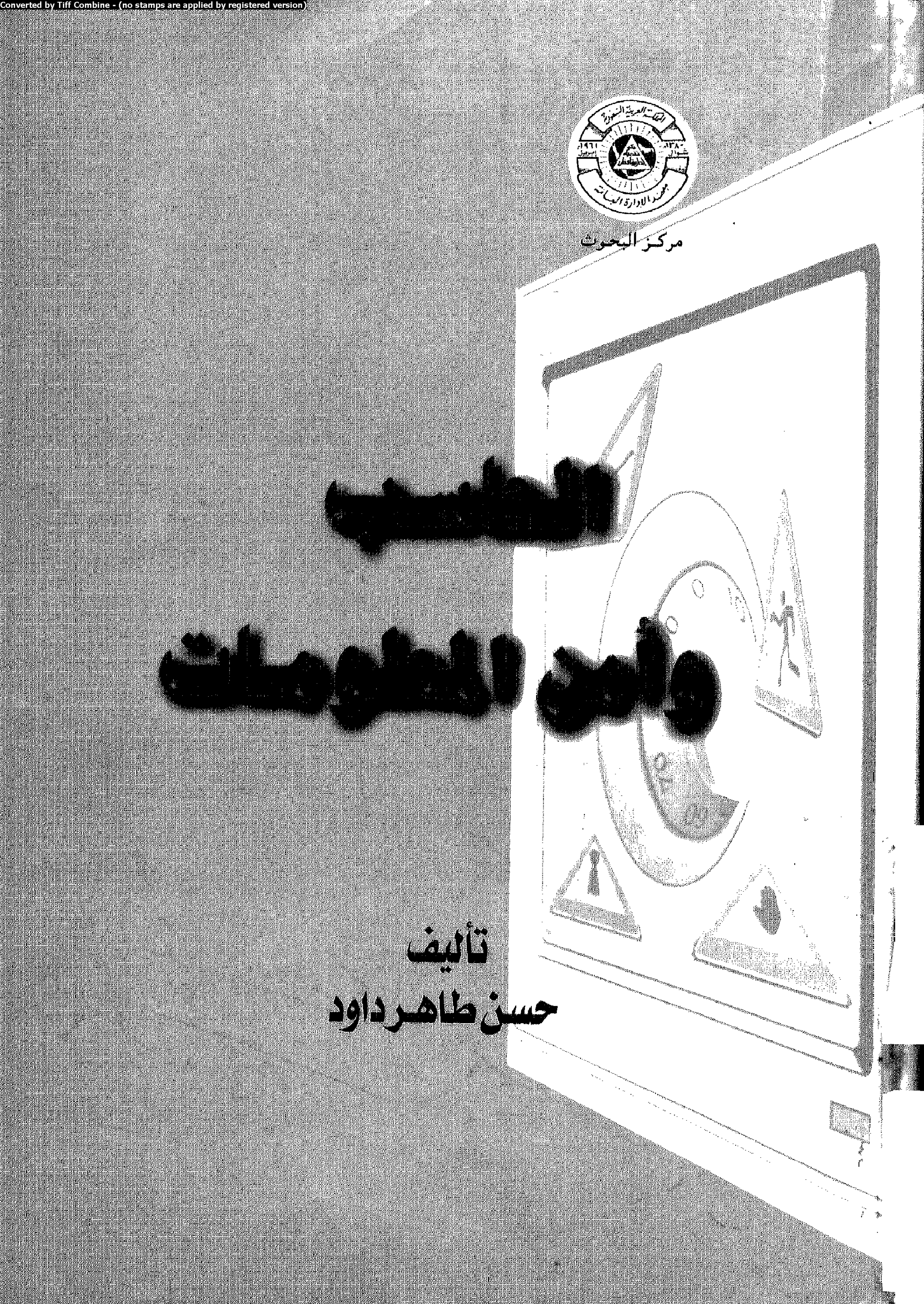

مركز البحوث
الحاسب
وأمن المعلومات
تأليف
حسن طاهر داود



بسم الله الرحمن الرحيم



مركز البحوث

الحاسب

وأمن المعلومات

حسن طاهر داود

١٤٢١هـ - ٢٠٠٠م

بطاقة الفهرسة

ح معهد الإدارة العامة ، ١٤٢٠هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

داود ، حسن طاهر

الحاسب وأمن المعلومات - الرياض .

٤٣٢ص ؛ ١٦,٥ × ٢٣,٥ سم

ردمك : ٨-٠٧٦-١٤-٩٩٦٠

١-أمن المعلومات ٢-الحاسبات الإلكترونية-إجراءات الأمن والسلامة

أ - العنوان

ديوي ٠٠٥,٨ ٢٠ / ٣٢٦٣

رقم الإيداع: ٣٢٦٣ / ٢٠

ردمك : ٨-٠٧٦-١٤-٩٩٦٠

إهــداء

" إلى رفيقة الدرب الطويل ..
التي جعلت من مسيرة الحياة
الشاقة رحلة ممتعــة "

حسن طاهر داود



محتويات الكتاب



مقدمـــــــة

الحمد لله والصلاة والسلام على رسول الله ..

"الحاسب" و"أمن المعلومات" كانا معًا المحوريـــن الرئيسيـــيين اللذيـــن أمضيت حياتي العملية معهما وبينهما. فكانا لي عملاً وهواية واحترافًا، بـــل وعشقًا، خلال العقود الثلاثة الماضية. ولذلك كنت أود دائمًا أن يـــأتي يـــوم أستطيع أن أتيح فيه هذه الخبرة المتواضعة للآخرين، ولذلك تمت ولادة هـــذا الكتاب "الحاسب وأمن المعلومات"، بعد مخاض طويل، ليطرق هذا الموضوع الهام والحيوي الذي يمس حياة الأفراد، كل الأفراد، كما يمس مصائر الدول، كل الدول.

رأيت أن أبدأ الكتاب بمقدمة لابد منها للموضوع ولذلـــك خصصـــت الفصل الأول للحديث عن "أمن المعلومات" وأهميته وأثر تطور التقنية علـــى الأمن، وعن ثورة المعلومات في العصر الحديث.

ثم تحدثت في الفصل الثاني عن "الأمن المادي لمراكز المعلومـــات"، فتحدثت عن أمن المنشآت، وأمن الأجهزة ووسائط المعلومات، وأمن الأفراد، وضربت أمثلة من الواقع عن الكوارث التي تنجم عن عدم الاهتمـــام بـــأمن المنشآت ، كما تحدثت عن الدور المهم الذي يلعبه ضابط أمن نظم المعلومات في المؤسسات المختلفة.

وخصصت الفصل الثالث للحديث عن "جرائـــم الحاســب" وأنواعـــها وبعض الأمثلة لها، كما تحدثت فيه عن بعض الأساليب الناجحة لمكافحة هذا النوع من الجرائم، وختمت هذا الفصل بالحديث عن التشريعات والقوانين في مجال مكافحة جرائم الحاسب ودعوت لأن تسن المؤسسات التشـــريعية فـــي الدول العربية قوانينها الخاصة بمكافحة جرائم الحاسب ولكي تقـــوم بتعديـــل قوانينها وتشريعاتها الحالية لتعكس التطور التقني الذي نشـــأ عـــن دخـــول الحاسب الآلي إلى حياتنا. وإذا شاء القارئ الحصـــول علـــى المزيـــد مـــن المعلومات عن هذا الموضوع فإنني أحيله إلى كتاب أكثر تخصصًـــا، وهـــو كتابي "جرائم نظم المعلومات" [داود ٢٠٠٠].

الفصل الرابع كان من المناسب أن أخصصه للحديـــث عـــن جريمـــة خطيرة من جرائم الحاسب وهي "فيروسات الحاسب". فتحدثت عـــن طبيعـــة الفيروسات ونشأتها وألقيت نظرة من الداخل عليها، ثم أوردت بعض طـــرق الوقاية من الفيروسات، وبعض طرق علاج آثارها إذا وقع المحذور.

في الفصل الخامس تحدثت عن موضوع "مواجهة الكوارث" وأن المهم عند حدوث الكارثة أن يستمر العمل وألا يتوقف، حتى لو تم يدويًـــا. كمـــا تحدثت عن الأخطار المحتملة والتي قد تسبب كوارث لبعض مراكز الحاسب الآلي، واختتمت هذا الفصل بالحديث عن المبادئ الأساسية لنجـــاح نشـــاط مواجهة الكوارث، وأنه يأتي على رأس هذه المبادئ ضرورة وجود خطـــة للطوارئ.

الفصل السادس تحدثت فيه عن "تحليل المخاطر" فقدمت فيه منهجيـــة جديدة أتمنى أن تتبعها مراكز الحاسب الآلي في تحليل المخاطر التي تخشـــى أن تتعرض لها، وتحدثت بالتفصيل عن هذه المنهجية المقترحـــة بمراحلـــها المختلفة: (١) تقييم أصـــول المؤسســـة. (٢) إدارة الأخطـــار. (٣) تقديـــر الخسائر. (٤) الأنظمة الحرجة. (٥) إجراءات حماية الأصول. (٦) البدائـــل الاحتياطية.

في الفصل السابع كان موعدنا مع موضوع أظن أنه على جانب كبـير من الخطورة وهو "خطة الطوارئ المعلوماتية"، فتحدثت عن أهــداف هــذه الخطة وما يمكن أن تحققه للمؤسسة من فوائد معنوية ومادية، وتحدثت عــن عوامل النجاح التي يجب أن تتوفر حتى تحقق الخطة أهدافها، وقدمت وصايا عشر للإدارة العليا تتعلق بالخطة، ثم حددت باختصار ما يجب أن تحتـــوي عليه الخطة من فصول وملاحق.

الفصل الثامن خصصته للحديث عن "تنفيذ خطة الطوارئ" ، لكي نبين الخطوات العملية اللازمة لوضع خطة الطوارئ موضع التنفيذ ، فتحدثت عن إجراءات الطوارئ، وفرق الطوارئ ومهام المشاركين فيها ، وأسلوب اختبار الخطة وتعديلها ومراقبتها، ثم أسلوب تدريب الموظفين على تنفيذ الخطة.

في الفصل التاسع تحدثت عن "تشفير البيانات" أو (تعميــة البيانــات)، فتوسعت في الحديث عن مفهوم التشفير وتاريخه وأهميته كوسيلة فعالة للغاية لتأمين البيانات. وتحدثت عن أنواع التشفير، بدءا من شفرة المفتاح الســري (شفرة قيصر)، وأشهر أنظمتها وهو نظام تشفير البيانات القياســي (DES)، فقمت بتقييم هذا الأسلوب وبينت كيفية كسر هذه الشفرة. ثم تحدثت بعد ذلــك عن التشفير باستخدام المفتاح العلني، وعن أشهر أنظمته وهو نظــام (RSA)، وأنهيت هذا الفصل بقسم عن أحدث وسائل التشفير وهو التشفير "المـــودع"، وعن استخدامه في تشفير المكالمات الهاتفية.

الفصل العاشر خصصته للحديث عن "نظم أمن البيانات"، وهي النظــم المتاحة في الأسواق والتي تكفل الأمن. فتحدثت عن دورها وإمكاناتها، وعن الموارد التي يجب حمايتها، والتقارير التي تنتجها هذه النظم، وأوردت بعض نظم البيانات المتاحة في الأسواق سواء للحاســب المركــزي أو الحاســبات الشخصية، وأوضحت كيفية المفاضلة بينها. تحدثت بعد ذلــك عــن النســخ الاحتياطي ومعدلاته وكيفية استعادة البيانات المفقودة، ثــم ختمــت الفصــل

بالحديث عن تصنيف مستويات مراكز الحاسب الآلي وفقًا لاتباعها لقواعــــد ومعايير أمن المعلومات.

في الفصل الحادي عشر تحدثت عن "أمن التطبيقات" وأثر بيئة العمــل على الأمن، ثم تحدثت بشيء من التفصيل عن المشاكل الأمنيــة فــي بيئــة "العميل / الخادم". واختتمت الفصل بالحديث عن كيفية تأمين التطبيقات عنــد استخدامها بواسطة الأجهزة المحمولة خاصة إذا تم الاتصال من خلال شــبكة الهاتف العامة.

يكاد الفصل الثاني عشر أن يكون امتداداً لسابقه، ولكني ركزت فيـــه على "أمن قواعد البيانات" ، فقدمت للقارئ غير المتخصص بعض المعلومات عن طبيعة استخدام قواعد البيانات، ثم أوضحت كيف يمكن وضـــع خطــة تأمين البيانات في بيئة عمل تستخدم قواعد البيانات، ومن منا لا يستخدمها!

في الفصل الثالث عشر انتقلت إلى موضوع جديد وهو "أمن شـــبكات نقل المعلومات" لما لهذا الموضوع من أهمية حيوية فائقة ، وقد امتد اهتمامي بهذا الموضوع ليشمل الفصول الثلاثة التالية. بل لعلني أذهب في القول إلـــى أن هذا الموضوع يحتاج إلى كتاب مستقل بذاته. في هــــذا الفصــل بــدأت بالحديث عن مفهوم الشبكات وأنواعها، والأجهزة المستخدمة فيها، والــبرامج التي تستخدم في مجال الشبكات، والأساليب الحديثة لنقل البيانات. ثم انتقلــت للحديث عن مصادر تهديد البيانات خلال مرورها بالشبكات ، وختمت الفصل بالحديث عن كيفية ضمان صحة البيانات المرسلة.

في الفصل الرابع عشر مضيت في الحديث عــن الشــبكات فتنــاولت موضوع الساعة وهو "أمن شبكات (إنترانت) المحلية" وهو الــهاجس الــذي يشغل بال الكثير من الشركات التي تستخدم "الإنترانت" في شبكاتها المحليــة. رأيت أن أبدأ الفصل بالتمهيد بتعريف الشبكات المحلية وأنواعها ومكوناتــها، ثم أوضحت مفهوم "إنترانت" والمقصود منها، ثـــم أوردت وســائل تــأمين المعلومات المتبادلة في الشبكات المحلية، وأمن البريد الإلكتروني.

الفصل الخامس عشر والأخير كان امتداداً لسابقيه ولكنـــه كـــان مـــن نصيب الوافد الجديد الذي أتى في نهاية القرن العشرين ليعيد تشـــكيل نمـــط الحياة على الأرض قبل ولوجنا من بوابة القرن الحادي والعشـــرين، أعنـــي بذلك الإنترنت. لذلك خصصت هذا الفصل للحديث عن "أمن شبكة المعلومات العالمية (إنترنت)"، فبدأت الفصل بالتعريف السريع بهذه الشبكة والمشـــاكل التي تكتنفها والأخطار الأمنية المحيطة بها على المستويين العالمي والعربي. وتحدثت بعد ذلك عن المستقبل وعن شبكة "إنترنت ٢" الجديدة. ثـــم انتقلـــت لتقنيات حماية المعلومات واستخدامها في شبكة (إنترنت) . وعند الحديث عن تقنيات الحماية كان لابد من الحديث عن "جدران الحمايـــة"، وعـــن مـــدى فاعليتها. واختتمت الفصل بموضوعين خاصين بالمملكة العربية الســـعودية هما أسلوب تنظيم استخدام شبكة "إنـــترنت" فـــي المملكـــة ودور الأجـــهزة السعودية المعنية بأمن المعلومات في ضمان أمن الشبكة. ثم أوردت قائمـــة بالمراجع التي استخدمتها في إعداد هذا الكتاب وهي حوالي أربعين مرجعًا.

وأود أن أشير إلى مشكلة واجهتني خلال إعداد الكتاب وهـــي مشـــكلة المصطلحات، حيث إننا في العالم العربي لم نتفق على ترجمة واحدة للعديـــد من المصطلحات العلمية، وكثير من هذه المصطلحات يظهر كل يوم، ولذلـــك فإنني، عند الاختلاف، كنت ألجـــأ إلـــى "معجـــم مصطلحـــات الحاســـبات الإلكترونية" الصادر عن مركز الأهرام للترجمة والنشر بالقاهرة حيث وجدته أكثر تحريًا لصحة الكلمات وصحة الاشتقاقات والبعد عـــن الغريـــب مـــن المصطلحات بقدر الإمكان، أما المصطلحات الحديثة جدًا، والتـــي لـــم تجـــد طريقها للمعاجم بعد فقد اجتهدت في وضع المقابل لها وأتمنى ألا أكون قـــد شططت كثيرًا في اجتهاداتي هذه.

اختتمت الكتاب بملحق أعتقد أنه مرجع هام في حد ذاته وهو تطبيـــق عملي لخطة طوارئ مقترحة تم إعدادها، بواسطة عدد من المتدربيـــن مـــن مديري مراكز الحاسب الآلي بالمملكة العربية السعودية وبعض الدول العربية

الشقيقة، ضمن برنامج "إدارة مراكز الحاسب الآلي" الذي قمت بتدريس بعض مواده. ولم يكن لي من جهد في إعداد هذه الخطة ســوى جـهد الإشــراف والتوجيه، مع إدخال بعض التعديلات الضرورية عند إعداد الكتــاب بــهدف اكتمال الفائدة.

أتمنى في النهاية أن ينظر القارئ، بعد الانتهاء من قراءة هذا الكتــاب، إذا لم يكن مملاً، أن ينظر إلى أمن المعلومات نظرة مختلفة، نظرة أكثر جدية وأكثر حرصًا، فأمن المعلومات قد يكون الفاصل بين النصر والهزيمة فـــي الحرب وقد يكون الفيصل بين البقاء والفناء لدول أو أفراد أو مؤسســـات أو شركات. وأتمنى بعد ذلك، وقبل ذلك، أن يكون هذا العمل خالصًا لوجــه الله تعالى، وأن يضعه سبحانه في ميزان حسناتي يوم القيامة.

المؤلف

الرياض

يناير ٢٠٠٠

الفصل الأول

أمن المعلومات

موضوعات الفصل:

(١) عصر المعلومات.

(٢) مفهوم أمن المعلومات.

(٣) خصوصية أمن الحاسب.

(٤) أثر التطور التقني على أمن المعلومات.

(٥) ثورة المعلومات في العصر الحديث.

(٦) أهمية أمن المعلومات للدول والمنظمات والأفراد.



يمثل هذا الفصل مقدمة ضرورية للكتاب حيث نتحدث فيه عن أمن المعلومات، فنبدأ الفصل بالحديث عن العصر الذي نعيشه (عصر المعلومات)، وظهور الحاسب الآلي وكيف أصبحت المعلوماتية هي السلاح النووي الجديد في يد الدول العظمى، ثم نبين أثر ثورة الاتصالات. ننتقل بعد ذلك إلى مفهوم أمن المعلومات ومحاولة إيجاد تعريف دقيق له، ثم نتحدث عن خصوصية أمن الحاسب. ونتحدث بعد ذلك عن أثر التطور التقني على أمن المعلومات وكيف أن فجوة التقنية ليست في صالح أمن المعلومات، وعن الوجه الآخر للتقنية الذي أبرز مشكلة الأمن، ثم نقترح إنشاء إدارة (ربما تتبع وزارة الداخلية) تعنى بأمن المعلومات، ثم نتحدث عن ثورة المعلومات في العصر الحديث. ونختتم الفصل بالحديث عن أهمية أمن المعلومات للدول والمنظمات والأفراد، ومن ثم نطرح السؤال: أين نحن من أمن المعلومات؟

١- عصر المعلومات

١-١- المعلومات كوسيلة للسيطرة

عصر المعلومات الذي نعيشه الآن هو عصر أصبحت المعلومات فيه هي المقياس الذي نقيس به قوة الشعوب، فمن يملك المعلومات في هذا العصر يستطيع أن يسيطر.. هكذا باختصار شديد. فالسيطرة لم تعد جيوشاً تغزو أو أساطيل تدك المدن أو عسكر يجوسون في شوارع الدول المحتلة، هذا النموذج من السيطرة لم يعد موجوداً هذه الأيام، فقد شهدت حقبة الستينيات من القرن العشرين زوال آخر مظاهر هذا النموذج من السيطرة الاستعمارية في العالم.

١-٢- عصر الحاسب

خلع الاستعمار إذًا عباءته العسكرية وارتدى عباءة اقتصادية . ولكن صادف أن هذا التحول التكتيكي قد ترافق مع تحول ضخم آخر غير الخريطة العلمية للعالم وقلب جميع الموازين وخلط كافة الأوراق وهو اختراع الحاسب الآلي. فقد ساعد هذا الاختراع ، الذي يمكن القول إنه يماثل اختراع الكهرباء في العصر الحديث أو اختراع النار في عصور ما قبل التاريخ، وأدى ظهور الحاسب إلى ارتفاع قيمة المعلومات في هذا العصر. وبارتفاع قيمة المعلومات وأهميتها وتزايد القدرة على استخدامها أصبحت توظف بذكاء للاستفادة منها اقتصاديًا، وأصبح الحاسب والمعلومات معًا في خدمة الاقتصاد. وكان من الطبيعي بعد ذلك أن تكتسب أهمية المعلومات بعدًا عسكريًا وسياسيًا.

هذا الاهتمام بالحاسب الآلي وعلومه واستخداماته لم يعد خافيًا على الدول العربية بصفة عامة فقد وجدنا خلال العقد الأخير من القرن العشرين كيف انتشر تدريس الحاسب في المدارس حيث بدأ دخوله في المدارس الثانوية ثم توسع استخدامه حتى أصبح مادة تدرس في المدارس الابتدائية ومراحل التعليم ما قبل الأساسي، وفي كثير من الدول العربية أصبحت مادة الحاسب الآلي تدرس ضمن مناهج جميع الكليات بلا استثناء.

١-٣- المعلوماتية سلاح نووي جديد

شيئًا فشيئًا تخلع الدول الاستعمارية العباءة الاقتصادية السافرة لتستخدم عباءة جديدة أكثر خطورة وأكثر جدوى نسجتها من هذا السلاح الجديد سلاح المعلومات. وشيئًا فشيئًا أخذ يتشكل ما يمكن أن نطلق عليه عصر المعلومات، أو عصر المعلوماتية إذا أردنا أن نختار تعبيرًا أكثر شمولاً إذ هو يضيف إلى المعلومات نفسها تلك الأدوات التي تعالج هذه

المعلومات وتستفيد منها. هذه الأدوات منها الحاسبات والأجهزة والتقنيات والبرامج التي تخدمها، كما إنه يضيف كذلك البيئة التي تستخدم هذه المعلومات بل والبشر الذين يقومون على خدمتها وإعدادها وتفعيلها.

المعلوماتية إذن هي السلاح النووي الجديد، الذي قد يفصل بين النصر والهزيمة في حالة الحرب، فمن يعلم سوف ينتصر حتى لو لم يكن هو الأقوى، ومن لا يعلم سوف ينهزم حتى لو كان هو الأقوى. إذ قال الله تعالى "**قُلْ هَلْ يَسْتَوِي الَّذِينَ يَعْلَمُونَ وَالَّذِينَ لاَ يَعْلَمُونَ** ... الآية" سورة الزمر آية رقم (٩).

ويظل الحاسب الآلي دائمًا هو ذلك السلاح الأقوى في عصر المعلومات وتلك الأداة التي لا غنى عنها. ولم تغب هذه الحقيقة عن الدول الكبرى، فنرى هذه الدول ترفض بيع أجهزة الكمبيوتر المتطورة لديها مثل السوبر كمبيوتر إلى الدول (غير الصديقة)، أو الدول التي تُخشى منافستها إما في سوق الاقتصاد أو في سوق السياسة، أو الدول التي يُظن أن لديها برامج للتسليح النووي، ذلك لأن الحاسبات المتطورة تسرع كثيرًا من معدل التقدم في هذه البرامج وتساعد على تنفيذها.

١-٤- ثورة الاتصالات

وبازدياد حجم المعلومات وكثافتها ازدادت الحاجة إلى تبادلها وإلى انتقالها من مكان إلى آخر، إما داخل المؤسسة الواحدة أو من مؤسسة إلى أخرى أو حتى بين الدول. وهكذا ظهر ما أطلقنا عليه ثورة الاتصالات وأخذ هذا الفرع من فروع الهندسة ينمو ويلتقي مع علوم الحاسب حتى ظهر مجال جديد هو الاتصالات الرقمية، وأخذ التطور في هذا المجال يزداد كل يوم. وظهرت شبكات المعلومات ووجدنا أنها انتشرت في كل مكان وامتدت كابلاتها وخطوطها تنقل كميات هائلة من المعلومات عبر الكرة الأرضية،

وانطلقت أقمار اصطناعية عديدة تحيط بالأرض من كل جانب لتسهل انتقال المعلومات دون الحاجة إلى مرورها في "الكابلات" أو بين أطباق "الميكروويف".

وأخيرًا جاءت آخر صرعات هذا الزمان (إنترنت) هدية القرن العشرين قبل أن يرحل لوريثه الحادي والعشرين. جاءت إنترنت إذن لتضع المعلومات على اختلاف أنواعها وكمياتها وأهدافها عند أنامل الجميع، فأصبح كل فرد الآن يستطيع عن طريق هذه الشبكة، التي يستخدمها الملايين، أن يحصل على ما يشاء من معلومات من مختلف أنحاء الدنيا في أي لحظة من ليل أو نهار.

٢- مفهوم أمن المعلومات

٢-١- سهولة التقاط المعلومات

إن المعلومات (تسري) من حولنا في كل مكان، هي إشعاعات في الجو تنتقل من طبق "ميكروويف" إلى آخر، وهي تصعد في الفضاء إلى قمر اصطناعي يدور في مداره لتنتقل إلى موضع آخر على هذه الأرض، وهي (تسري) في كوابل ممتدة عبر المدن أو عبر المحيطات، وهي حزم رسائل تنطلق من ركن إلى آخر في هذه المعمورة، ويستطيع أي شخص (إذا كان مسلحًا بالوسيلة والمعرفة) أن يصل إلى هذه المعلومات. فما هي الأخطار التي تهددها؟ وكيف نحميها؟ وكيف نضمن سلامتها؟ وكيف نتصرف إذا وقع المحذور؟ هذه الأسئلة كلها هي التي يحاول هذا الكتاب المتواضع في فصوله القادمة أن يقدم الإجابة عنها.

أمن المعلومات قضية ساخنة باستمرار وقد أثبتت أهميتها الفائقة في السنوات الأخيرة بالذات، فمنذ عشر سنوات فقط كنا إذا أثرنا موضوع

"الأمن" في مجال المعلومات (أو الحاسبات بالذات) كنا نسمع من يقول إن الأمن ليس مشكلة تبحث عن حل وإنما هو حلول تبحث عن مشكلة !. ولكن هذه المقولة لم يعد لها وجود الآن بعد التطور الكبير الذي شهدته التقنية في السنوات الأخيرة ، فمستخدم الحاسب اليوم، نتيجة لهذه التطورات، أصبح من الممكن أن يكون "أي شخص" وبيئة التشغيل التي يتم فيها تشغيل برامج الحاسب أصبح من الممكن أن تكون "أي مكان".

٢-٢- تعريف أمن المعلومات

نستطيع الآن أن نحدد التعريف التالي لأمن المعلومات:

يقصد بأمن المعلومات حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة. ويتم ذلك عن طريق اتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات وهي الكنز الثمين الذي يجب على المنشأة الحفاظ عليه.

٣- خصوصية أمن الحاسب

٣-١- المعلومات في عصر الحاسب

إذا ذكرت المعلومات في هذا العصر فلابد أن يذكر الحاسب (أو الحاسوب)، إذ هو الوسيلة التي ابتكرها الإنسان للحصول على المعلومات وتبويبها وتصنيفها وتخزينها. فالحاسب والمعلومات إذًا أصبحا صنوان متلازمان، وأصبح الحاسب هو مصدر المعلومات وأصبح هو أيضًا مقصدها. ولذلك كان هذا الكتاب الذي يتحدث عن هذه العلاقة الوثيقة بين

الحاسب (المصدر والمقصد) وبين المعلومات وأمنها وسلامتها وهو الهدف الذي يسعى إليه كل من بحوزته معلومات.

٣-٢- المعلومات في عصر الشبكات

انتشر في الآونة الأخيرة استخدام شبكات المعلومات مع ما صاحب ذلك من الزيادة المطردة في نطاق الترددات بالنسبة لخطوط الاتصالات المستخدمة لبث المعلومات، بالإضافة إلى ازدياد سرعات البث الآمنة إلى معدلات هائلة في الوقت الحالي مما يساعد في الحصول على المعلومات في زمن قياسي. ونتج عن ذلك إمكان نقل كمية كبيرة من المعلومات في زمن قصير للغاية، فأصبحت الآن عملية بث كمية كبيرة من المعلومات من الممكن أن تتم في مدة لا تتجاوز بضع دقائق، هذه الكمية نفسها من المعلومات كان يستغرق بثها في الماضي ساعات عديدة مما سهل كثيرًا من مهمة الجواسيس وقراصنة المعلومات، وجعل مهمة مكافحة التجسس وانتهاك سرية المعلومات أكثر صعوبة.

٤- أثر التطور التقني على أمن المعلومات

تشهد تقنية المعلومات تطورات هائلة هذه الأيام، فلا يكاد يمر يوم إلا وهناك جديد في مجال التقنية فأجهزة الحاسب في تطور مستمر لا يتوقف، وسرعات تشغيل البرامج فيها، سواء كانت شخصية أو متوسطة أو كبيرة، تصل إلى آفاق ما كنا نظن أنها تصل إليها ، وطاقات تخزين المعلومات على الأقراص الممغنطة تزداد كل يوم في تنافس محموم بين شركات الحاسب، وسرعة الوصول إلى هذه المعلومات في تطور مستمر، ناهيك عن قدرات ذاكرة الحاسب، تلك القدرات التي تتعاظم شهرًا بعد شهر. ويتواكب مع هذا التطور المطرد في العتاد (Hardware) تطور موازٍ في البرمجيات

(Software)، فنجد الشركات تتسابق في إنتاج لغات برمجة جديدة أكثر سهولة للمستخدم وأكثر كفاءة في قوة المعالجة. أضف إلى كل ذلك هذا الانتشار المتزايد لشبكات المعلومات التي نراها الآن تطوي المسافات بين الدول وتشمل العالم كله جاعلة منه قرية صغيرة، وساعد على ذلك تطور تقنيات الشبكات وأجهزة الاتصال، وتظهر لنا النقاط التالية التي تستحق منا وقفة للدراسة:

٤-١- فجوة التقنية ليست في صالح أمن المعلومات

كان للتطور المتلاحق والسريع لتقنيات الحاسب آثاره الملحوظة على أمن الحاسبات سواء سلباً أو إيجاباً ، ولكن الأمر الملاحظ بصفة عامة هو أن ذلك التطور السريع يكون في غالب الأحوال أسرع من أن تتم ملاحقته بواسطة خبراء أمن الحاسبات لتغطية الثغرات التي قد تنشأ عن النظم الجديدة الأكثر تعقيدًا، مما يتسبب دائماً في وجود فجوة تقنية، من الصعب ملؤها، بين السلاح التقني المستخدم في انتهاك المعلومات وبين الأسلحة المضادة التي يلجأ إليها خبراء أمن المعلومات، هذه الفجوة من المؤكد أنها ليست في صالح أمن المعلومات وإحكام الحماية ضد انتهاكها.

٤-٢- الإقامة في قلعة الأمن المحصنة يجب أن تكون سهلة وممكنة وممتعة

الأمر الذي يجعل من قضية الأمن قضية ساخنة ودقيقة في الوقت نفسه هو أن وضع الإجراءات الأمنية المحكمة لحماية البرامج والبيانات وباقي موارد الحاسب ليس هو الأمر المهم، وإنما المهم هو أن تكون هذه الإجراءات عملية وميسرة. فمن السهل على أي شخص أن يبني قلعة مسلحة محكمة التحصينات، ولكن من الصعب أن نجعل الإقامة في هذه القلعة سهلة وممكنة وممتعة لسكانها.

٤-٣- الأمن مشكلة تهم الجميع

يتضح مما سبق أن أهمية قضية الأمن ازدادت هذه الأيام فأصبحت كما ذكرنا من قبل مشكلة تبحث عن حل، وأصبحت هذه القضية تهم رجال الأعمال والمدير وكل من لديه معلومات، وأصبحت تهم المستفيد العادي، وتهم الشركات التي تقدم خدمات المعلومات، وتهم مصممي النظم والتطبيقات، وكذلك الشركات المطورة للأجهزة والبرمجيات، بل هي تهم في الوقت نفسه رجال القانون والتشريع ورجال الأمن، وتهم متخصصي الاتصالات، وتهم المدرسين والطلاب، وتهم مسئولي الرقابة، سواء الرقابة المالية أو الرقابة الإدارية، بل هي مهمة كذلك للصحفيين، وعلى رأس هؤلاء جميعًا يأتي مسئولو أمن المعلومات كمهتمين رئيسيين بهذه القضية. أي أنها باختصار تهمنا جميعًا، وهذا هو ما أعطى نظم أمن المعلومات، تلك النظم التي تكفل الأمن لبياناتنا، أهمية قصوى في عالم اليوم.

٤-٤- الوجه الآخر للتقنية

سوف نحاول أن نرصد فيما يلي بعض مجالات التطور التقني التي أبرزت مشكلة الأمن وزادتها حدة وسخونة:

٤-٤-١ تشغيل البرامج أصبح ممكنًا في بيئات بعيدة

سمح الاتجاه إلى نظم التشغيل الموزعة (Distributed Systems) بتشغيل المواقع البعيدة جغرافياً بمستوى عالٍ من الكفاءة، فأصبح من الممكن تشغيل البرنامج فعلياً في بيئة عمل أخرى أو في مركز حاسب آخر، فأنت تستطيع أن ترسل برنامجك ليتم تنفيذه على حاسب بعيد قابع في أحد

المراكز، التي ربما لا تعرفها، الأمر الذي خلق مصادر تهديد جديدة لم تكن معروفة من قبل، فأنت لا تضمن (براءة) هذه البرامج التي تستضيفها دون أن تدري في حاسبك، ولا يمكنك التأكد من حسن نواياها.

٤-٤-٢- قواعد البيانات العالمية أصبحت في متناول اليد

أصبح من المألوف الآن أن تتعامل البرامج مع بيانات موجودة في أماكن بعيدة، وأصبح الدخول إلى قواعد البيانات العالمية في أي مكان من العالم والحصول منها على المعلومات أمرًا سهلاً ومتاحًا، وقد انتشر هذا الأسلوب بكثرة في الآونة الأخيرة ، مع ما يصاحب هذه التسهيلات من زيادة احتمالات انتهاك المعلومات، ففي بعض الأحيان قد لا يكون من السهل أن تسيطر على من يدخلون إلى قاعدة البيانات الخاصة بك أو أن تتحكم فيما يصلون إليه من معلومات.

٤-٤-٣- لم يعد المتخصص هو القادر الوحيد

ظهرت في السنوات الأخيرة لغات برمجة حديثة سهلة الاستخدام، وبعضها موجه إلى المستخدم العادي ولا يحتاج استخدامها إلى خبرة كبيرة. وقد أدى ظهور هذه اللغات إلى وضع قوة المعالجة (أو الحوسبة) في أيدي أعداد كبيرة من المستفيدين مما جعل عملية الحصول على المعلومة عملية سهلة، خاصة مع ظهور لغات للاستفسار يمكن بواسطتها استخراج المعلومات والإحصاءات المطلوبة بسهولة من قواعد البيانات. أي أن الشخص العادي يستطيع الآن البرمجة ويستطيع البحث في قواعد البيانات، وربما أتاح له ذلك الاطلاع على معلومات محظورة، فضلاً عن احتمالات تعديل هذه المعلومات أو تدميرها.

٤-٤-٤- صعوبة السيطرة على تسرب المعلومات في زمن المؤتمرات عن بعد

في السنوات الأخيرة وبعد ظهور (الشبكات الرقمية للخدمات المتكاملة Integrated Services Digital Networks) وإمكاناتها الواسعة ، أصبح من الممكن نقل الصوت والصور والرسوم وأفلام "الفيديو" بسهولة عبر هذه الشبكات. كما أصبح من الممكن الآن وبنفس السهولة عقد ما نطلق عليه "المؤتمرات عن بعد" أو (Remote Conferencing)، وهذا التطور جعل الرقابة على خروج المعلومات من الدولة، أي دولة، أو مراقبة دخول هذه المعلومات إليها ضربًا من المستحيل.

٤-٤-٥- "الماوس" يحرك "الكاميرا" التليفزيونية في أقصى الأرض

رأينا ضمن التطورات التقنية الأخيرة كيف أنه من الممكن زرع "كاميرا" تليفزيونية في أي مكان لتبث الصور التي تلتقطها بشكل متواصل، وكيف أنه يمكن استقبال هذا البث من أماكن بعيدة. ورأينا كيف يمكن استخدام نفس التقنية كإجراء وقائي، فتوجد الآن "كاميرات" تليفزيونية يمكن توجيهها عن بعد عن طريق الهاتف فيمكن زرع هذه الكاميرا في المكان المطلوب مراقبته ثم توجيهها عن بعد، ربما من مدينة أخرى، باستخدام الماوس الخاص بجهاز حاسب شخصي متصل بالهاتف، ويمكن أيضًا بواسطة الهاتف الحصول على هذه الصور الملتقطة بحيث تعرض على شاشة الحاسب، والأهم من ذلك أن هذه العملية يمكن أن تتم من دولة أخرى، في أقصى الأرض، عن طريق شبكة إنترنت !!

الوجه الآخر لهذه التقنية، شأنها شأن غيرها من التقنيات الحديثة، هو أنها يمكن أن تستخدم من جانب أجهزة التجسس التابعة للدول أو الشركات الصناعية أو غيرها.

وتستخدم هذه التقنية من جانب لجنة الأمم المتحدة للتفتيش على الأسلحة في العراق.

٤-٥- إدارة أمن المعلومات

يتضح من العرض السابق كيف ازداد مؤخرًا حجم الثغرات الأمنية التي يجب على خبراء أمن الحاسبات معالجتها، كما يتضح مدى العبء المتزايد الملقى على كاهلهم، ويتم علاج هذه الثغرات إما بتطوير إجراءات تأمين الحاسبات واستخدام التقنيات المضادة لهذا الغرض، أو بإصدار تشريعات خاصة تتيح حماية المعلومات وردع كل من يحاول انتهاكها، أو بالاثنين معًا.

لذلك نقترح هنا إنشاء إدارة لأمن المعلومات، ربما كانت وزارة الداخلية مكانًا مناسبًا لها، بحيث تكون هذه الإدارة هي الراعي لأنشطة وأبحاث خبراء أمن المعلومات وتكون هي الأداة التي يمكن من خلالها تحقيق المعادلة الصعبة ونعني بها كيف يمكن ضمان أمن المعلومات بالشكل المطلوب في الوقت الذي نضمن فيه حرية الباحثين ومستخدمي المعلومات وعدم تكبيلهم بالإجراءات الأمنية، أي أن نجعل القلعة حصينة ونجعلها ــ في نفس الوقت ــ مريحة لسكانها.

٥- ثورة المعلومات في العصر الحديث

نحن نعيش هذه الأيام بحق عصر المعلومات، فالمعلومات اليوم أصبحت من أهم الموارد في المجتمع. ويظن بعض الباحثين أن الحجم الكلي للمعلومات في العالم كان قبل دخول الإنترنت إلينا، أو قبل دخولنا إليها، يتزايد بمعدل ١٢% سنويًا [Daler 1989] ولعل هذه النسبة اليوم وبعد انتشار الشبكة تكون أكبر بكثير. وهذا المعدل الهائل ــ لتزايد المعلومات في العالم ــ يجعل عملية معالجتها واستخلاص المفيد منها أمرًا صعبًا وتتزايد صعوبته عامًا بعد آخر.

بازدياد كم المعلومات وبازدياد حركتها (انتقالها من مكان إلى آخر

خلال الشبكات المحلية وعبر الشبكات الكبيرة وفي العالم كله من شرقه إلى غربه عبر شبكة الإنترنت)، بازدياد الكم والحركة أصبح أمن المعلومات في خطر، فهي دائمًا معرضة لأخطار عديدة ليس أقلها ضياع المعلومة أو تغيير مضمونها، وليس أخطرها اطلاع الغير عليها، فالأشياء الثمينة والنادرة والهامة تكون دائمًا عرضة لمحاولات الآخرين الوصول إليها لاقتنائها أو إتلافها، والمعلومات من هذه الأشياء الثمينة في كل عصر.

٦- أهمية أمن المعلومات للدول والمنظمات والأفراد

٦-١- أهمية أمن المعلومات

تنبع أهمية أمن المعلومات من أنها تستخدم من قبل الجميع بلا استثناء.. الدول والشركات والأفراد، كما أنها هدف للاختراق من جانب الجميع كذلك وأيضًا بلا استثناء .. الدول والشركات والأفراد، وفي بعض الأحيان تكون المعلومات هي الفيصل بين النصر والهزيمة في الحروب، وأحيانًا تكون هي الفيصل بين المكسب والخسارة للشركات وقد تكلف الفرد ثروته وربما حياته في بعض الأحيان.

وفي هذا العصر بالذات انقلبت الآية ولم تعد مشكلة الناس الحصول على المعلومات، وإنما أصبحت مشكلتهم هي هذا الفيض الهائل من المعلومات وكيف نفرق بين الغث منها والثمين. ومن ثم كيف نحمي هذه المعلومات من الأخطار التي تتهددها.

٦-٢- صناعة أمن المعلومات

صناعة أمن المعلومات تتزايد تقنياتها ومجالاتها يومًا بعد يوم، وتزدحم الأسواق بمنتجاتها، فيوجد الآن على سبيل المثال أكثر من خمسين شركة في العالم توفر برمجيات (جدار الحماية Firewall)، وهذه مجرد

تقنية واحدة من تقنيات أمن المعلومات. هذه التقنيات تضم كذلك العديد من برمجيات تشفير المعلومات (تعميتها) وأدوات التشفير وتقنيات (التوقيعات الرقمية Digital Signatures)، هذا فضلاً عن (البوابات Gateways) وأجهزة (توزيع الخدمة Servers) وبرمجيات تنظيم ومتابعة كلمات السر وبرمجيات مكافحة الفيروسات وغيرها كثير. وتؤكد المنافسة الحامية في الأسواق مدى اهتمام صناعة أمن المعلومات بمحاولة جذب انتباه العملاء، خاصة أولئك الذين يتعاملون مع شبكة إنترنت، ومن ذا الذي لا يتعامل معها!

٦-٣- أين نحن من أمن المعلومات ؟

هل أصبحت المعلومات في عالمنا اليوم أقل أمناً؟ هل تتخذ الحكومات والمؤسسات والأفراد الإجراءات الأمنية المناسبة للمحافظة على معلوماتها؟ هل تعرف جميع هذه الأطراف القيمة الدقيقة لكل من المعلومات التي لديها؟ وهل لديها جميعًا البديل الجاهز في حالة تعرض هذه المعلومات للخطر؟ يحاول هذا الكتاب في فصوله القادمة إلقاء الضوء على هذه القضايا كلها.



الفصل الثاني

الأمن المادي لمراكز المعلومات

موضوعات الفصل:

(١) أمن المنشأة.

(٢) أمن غرفة تشغيل الحاسب.

(٣) أمن الأجهزة.

(٤) أمن وسائط المعلومات.

(٥) أمن الأفراد.

(٦) دور ضابط أمن نظم المعلومات.



نقدم في هذا الفصل موضوع الأمن المادي لمراكز المعلومات، فنتحدث في البداية عن أمن المنشأة، والأخطار التي يتعرض لها مركز الحاسب في المنشأة، وأساليب الحماية العامة للمبنى، والوقاية ضد الحريق، وحماية الخدمات الأساسية، مثل: الطاقة الكهربائية والاتصالات الهاتفية وتكييف الهواء، وكيفية حماية المباني المزدحمة، ونقدم مجموعة من الأمثلة الواقعية، من مختلف بلاد العالم، عن الكوارث التي وقعت بسبب عدم الاهتمام بتطبيق قواعد حماية المنشآت. ونتحدث كذلك عن تجربة "هونج كونج" في تأمين المعارض . ننتقل بعد ذلك إلى الحديث عن أمن غرفة تشغيل الحاسب، وأمن أجهزة الحاسب المختلفة، وأهمية إيجاد موقع بديل يستخدم عند الحاجة، ثم نتحدث عن أمن وسائط المعلومات من أقراص وأشرطة وغيرها. نتحدث بعد ذلك عن أمن الأفراد، ثم نختتم الفصل بالحديث عن وظيفة مهمة للغاية وهي وظيفة ضابط أمن نظم المعلومات.

١- أمن المنشأة

١-١- أسئلة لابد من الحصول على إجابات عنها

قبل الدخول في تفاصيل تأمين أي منشأة يجب أن نحاول الإجابة عن مجموعة من الأسئلة لا يمكن البدء في إجراءات تأمين المنشأة دون الحصول على إجابات دقيقة عنها حيث إن اتخاذ القرار بالمفاضلة بين العديد من الخيارات يتوقف على دقة وصحة الإجابة، هذه الأسئلة هي:

١) ماذا نحمي؟ .. أي ما هي الموارد التي نسعى لحمايتها؟
٢) نحمي ضد من؟ .. أي ما هي الأخطار التي يجب مواجهتها؟
٣) ما مدى أهمية التأمين؟ .. أي ما هي الأضرار التي ستنجم عن فقد هذه الموارد؟
٤) إلى أي مدى يمكن أن ننفق على برامج الحماية؟

وهذا السؤال الأخير تتوقف إجابته على ثلاثة عوامل:

- مدى حساسية الموارد المطلوب حمايتها.
- درجة احتمال وقوع الأضرار.
- مدى جسامة الأضرار المتوقعة.

١-٢- الأخطار المادية التي يتعرض لها مركز الحاسب

من أهم الأخطار المادية التي يتعرض لها مركز الحاسب في المنشأة ما يلي:

١) الحريق.
٢) انقطاع الإمداد بالطاقة الكهربية.
٣) الإغراق بالمياه.
٤) انقطاع الاتصالات.
٥) الإهمال.
٦) الاقتحام.
٧) التخريب.
٨) السرقة.

١-٣- أساليب حماية المنشأة

حماية المنشآت موضوع كبير وهام ولا يمكن أن نحيط به في كتاب يركز على الحاسب الآلي، ولذلك سنركز على أساليب الحماية التي تخص نشاط الحاسب الآلي في المنشأة وتأمين هذا النشاط وحمايته من الأخطار المختلفة التي عادة ما تهدد هذا النشاط، هذه الأساليب نصنفها كما يلي:

- الحماية العامة للمبنى.
- الوقاية ضد الحريق.
- حماية الخدمات الأساسية.
- حماية المباني المزدحمة.

١-٣-١- الحماية العامة للمبنى

يجب اختيار موقع مبنى الحاسب بعيدًا عن الأخطار البيئية المحتملة، ويجب العناية بتحديد أماكن كل من: خزانات المياه، دورات المياه، وخزانات الوقود والتي يمكن أن ينشأ عنها أخطار كبيرة إذا لم يتم اختيار أماكنها بعناية كبيرة. كما يجب استخدام مواد مقاومة للحريق عند البناء.

يجب تحديد مناطق العمل وعزلها، واستخدام البطاقات الشخصية للموظفين وللزائرين عند التنقل، مع ضرورة وجود أبواب حاكمة عند الدخول إلى المناطق الحساسة تستخدم فيها البطاقات الممغنطة، أو الأقفال الرقمية، أو غيرها من وسائل التحقق من الشخصية.

وتلجأ بعض المنشآت إلى طلاء أسفل الجدران في كل قسم أو إدارة بلون معين، كالأحمر أو الأخضر أو الأصفر. وموظفو كل قسم يحملون على صدورهم بطاقات تحمل، بالإضافة إلى الاسم والصورة، دائرة صغيرة ملونة بنفس اللون المخصص للقسم. وكذلك زوار المبنى الذين يقصدون قسمًا معينًا يطلب منهم تعليق بطاقة زيارة تحمل لون القسم الذي يريدون زيارته. وذلك يجعل من السهل معرفة أي موظف أو زائر متواجد في مكان لا يجب أن يكون متواجدًا فيه. وإذا تطلبت طبيعة عمل أحد الموظفين (أو الزائرين) التواجد في أكثر من قسم يتم وضع أكثر من لون على بطاقته. وهكذا بنظرة واحدة، ومن مسافة بعيدة، يسهل التأكد من أي مخالفة.

١-٣-٢- الوقاية ضد الحريق

هذه النصائح يجب الالتزام بتنفيذها بكل دقة لتفادي نتائج الحريق وتقليل الخسائر إلى أكبر حد ممكن:

١) استخدام المواد المقاومة للحريق كلما أمكن ذلك.

٢) منع التدخين في الأماكن الحساسة.

٣) المحافظة على نظافة فتحات التهوية والتكييف.

٤) العناية بتخزين المواد القابلة للاشتعال.

٥) استخدام خزائن واقية ضد الحريق لوسائط تخزين البيانات.

٦) استخدام مفاتيح عازلة للأجهزة الكهربية.

٧) يفضل استخدام مادة (MS40) أو غاز الهالون كوسيلة إطفاء.

٨) استخدام وسائل اكتشاف الحريق والإنذار بحدوثه، واختبارها دوريًا.

١-٣-٣- حماية الخدمات الأساسية

الخدمات الأساسية التي يؤثر تعطلها بشكل كبير على أداء الحاسب الآلي بالمنشأة يجب أن تولى عناية كبيرة وهذه الخدمات من أهمها:

١) **مصدر الطاقة الكهربية**

- يجب استخدام مصدر يضمن استمرار الإمداد بالطاقة (UPS) واختبار وصيانة البطاريات الخاصة بهذا المصدر باستمرار.
- استخدام مولدات احتياطية لتوليد الكهرباء، واختبار كفاءة هذه المولدات دوريًا، وتأمين مصادر الوقود اللازمة لها.

٢) الاتصالات الهاتفية

- الصيانة المستمرة للخطوط الخاصة (Dedicated lines) .
- استخدام خطوط اتصال بديلة، فيمكن استخدام الخطوط "المراقمة" (dial-up) في حالة تعطل الخطوط الخاصة.
- استخدام أجهزة "مودم" بديلة تحسبًا لتعطل أي من هذه الأجهزة.
- استخدام مسارات بديلة تمر بها الرسائل في حالة تعطل بعض الخطوط.
- تأمين خطوط الاتصال ضد التنصت، أو التداخل، أو احتمالات التخريب.
- دراسة الوقت اللازم لتأمين خطوط بديلة في حالة تعرض الخطوط المستخدمة للتعطل لمدة طويلة.

٣) تكييف الهواء

- الصيانة المستمرة لوحدات التكييف، ومواسير المياه المستخدمة للتبريد.
- إعداد وحدات تكييف بديلة.
- دراسة الوقت اللازم لاستبدال وحدات التكييف في حالة تعطلها.

١-٣-٤- حماية المباني المزدحمة

١) المشكلة

عبر سنوات طويلة كان تحقيق الأمن في الأماكن العامة المزدحمة التي يؤمها عدد كبير من الزائرين يشكل مشكلة حقيقية تواجه المسئولين عن أمن هذه المناطق التي تشمل المعارض التي يزورها جمهور كبير، أو المصالح الحكومية المجمعة في مبنىً واحد أو منطقة واحدة، أو المؤتمرات

الكبرى التي تنعقد في أحد الفنادق على سبيل المثال.

كان من الضروري لضمان الأمن في هذه الأماكن أن يتعرض الداخل إليها للتفتيش ولفحص بيانات هويته، وحتى هذه الإجراءات لم تكن كافية لتحديد هوية مرتكب الجريمة في حالة وقوعها أو تحديد هوية الإرهابيين في حالة ارتكابهم عملاً إرهابيًا أو احتجازهم بعض الرهائن مثلاً، كما أنه في حالات الحرائق أو الدمار الواسع التي قد يتعرض لها المبنى كان من الصعب تحديد هوية الجثث التي ربما تكون قد تفحمت واستحال التعرف على أصحابها. وكان السبب وراء هذه الصعوبات كلها أنه لم تكن هناك وسيلة لتحديد الأماكن التي تردد عليها كل زائر مثل الأجنحة المختلفة في المعرض أو الإدارات المختلفة في المبنى الحكومي ، ومتى تمت هذه الزيارة ومتى غادر الزائر هذا الجناح أو هذه الإدارة والوقت الذي أمضاه في تلك المنطقة، فلكي يمكن تحقيق ذلك كان لابد من تعيين رجل أمن لكل زائر، وهذا بالطبع أمر مستحيل.

٢) الحل

في هونج كونج تمت تجربة نظام حاسب جديد لتسجيل ومتابعة زوار أحد المعارض التي أقيمت في أبريل عام ١٩٩٧م. وفي هذا النظام يقوم موظف الاستقبال بتسجيل بيانات الزائر بمجرد وصوله من واقع هويته وإدخال هذه البيانات إلى الكمبيوتر، ثم يقوم الكمبيوتر بعد ذلك بإخراج بطاقة مطبوعة تحمل (شفرة الخطوط Bar code) بحيث تحمل هذه البطاقة كافة بيانات الزائر، ويحتفظ الزائر بهذه البطاقة خلال تجواله في المعرض. وعند دخول الزائر لأي جناح في المعرض يتم تعريض هذه البطاقة "لماسحة" إلكترونية (Scanner) مرتبطة بالحاسب المركزي الموجود بالمعرض، وبمجرد قراءة الماسحة لبطاقة الزائر يتم إرسال إشارة إلى الحاسب المركزي تفيد زيارة الزائر لهذا الجناح أو تلك المنطقة والتوقيت الذي تمت فيه هذه

الزيارة، وعند خروج الزائر يتم تعريض البطاقة للماسحة مرة أخرى لتسجيل واقعة الخروج. وبذلك يتم بدقة تحديد المدة التي قضاها الزائر في كل منطقة من مناطق المعرض وكذلك تحديد الأشخاص الذين كانوا موجودين في منطقة محددة في لحظة معينة.

يحقق هذا النظام فوائد أخرى جانبية فهو مفيد من الناحية الإحصائية إذ أنه يؤدي إلى الحصول على إحصاءات دقيقة عن عدد الزوار لكل جناح ومتوسط المدة التي يقضيها الزائر في الأجنحة المختلفة بما يعكس اهتمامات الزوار وموضوعات تركيزهم، وبما يحدد نسب الإقبال على الأجنحة المختلفة بالمعرض.

وقد تم تطوير هذا النظام لاحقًا واستخدامه في معرض الإلكترونيات الذي أقيم في هونج كونج في شهر أكتوبر ١٩٩٨م. ومحور هذا التطوير كان إضفاء مزيد من الآلية عليه حتى لا يُضيِّع الزوار وقتًا عند الدخول أو الخروج من الأجنحة المختلفة.

ونعتقد أن هذا النظام يفتح الباب لتطورات وإضافات أخرى في المستقبل منها:

أن يتم استخدام نظم متطورة لقواعد البيانات ونظم حديثة للاستفسار بحيث يمكن الاستعلام في أي لحظة عن وجود شخص معين في المبنى وذلك عن طريق الاستفسار من الحاسب الآلي عن مكان تواجده، فيقوم الحاسب بتحديد المنطقة التي يتواجد فيها هذا الشخص بشكل فوري حتى يتسنى الاتصال به، أو ربما للتحذير من خطورته أو توجيه رجال الأمن لمراقبته في حالة ما إذا تلقت إدارة المبنى أو المسئولون عن الأمن فيه تحذيرًا معينًا يحذر من أحد الأشخاص مثلاً.

ربما أمكن في المستقبل الاستفادة من هذا النظام في التعرف على جثث القتلى الذين قد يسقطون ضحايا لحريق أو تدمير للمبنى، أو التعرف على شخصيات الرهائن والإرهابيين في الحوادث الإرهابية.

نتوقع كذلك أن يشهد المستقبل القريب تطورات أكثر إيجابية فمن الممكن أن يتم ربط الحاسب المركزي الموجود بالمبنى والذي يضم بيانات الزوار عند دخولهم بأحد الحاسبات الأمنية المركزية التي تضم بيانات عن مواطني الدولة جميعهم والذي يضم بيانات عن الجماعات الإرهابية وأفرادها والمشتبه فيهم كالحاسب الخاص بوزارة الداخلية مثلاً، حيث يتم أولاً بأول تدقيق بيانات الزوار بمجرد إدخالها للتثبت من صحتها، وربما وضع إدخال هذه التقنية وتعميمها نهاية للكثير من الحوادث الإرهابية.

١-٤- أمثلة لبعض الكوارث

١) كارثة "درنكة"

ذكرت وكالات الأنباء حادثة مفزعة عن قرية "درنكة" وهي إحدى قرى الصعيد في جنوب جمهورية مصر العربية حيث كانت القرية تقبع في سفح الجبل (تل مرتفع)، وعلى قمة هذا التل توجد خزانات لوقود الطائرات (وقود ذو طاقة احتراق عالية)! وفي إحدى ليالي الشتاء العاصفة من عام ١٩٩٦م ضربت المنطقة عواصف رعدية شديدة مصحوبة بأمطار غزيرة، وضربت إحدى الصواعق خزانات الوقود فانفجرت واشتعل الوقود وسالت كميات الوقود الهائلة مشتعلة بالنيران وانسابت على جوانب الجبل حتى وصلت إلى سفحه حيث تقع القرية الآمنة وسكانها نائمون. ومما زاد من الآثار المدمرة للكارثة أن مياه الأمطار كانت هي وسيلة النقل التي حملت النيران المشتعلة إلى بيوت القرية فأغرقتها وأحرقتها!! من المسئول عن هذه الكارثة؟! الجواب هو الاختيار الخاطئ لموقع خزانات الوقود أو موقع بيوت القرية أيهما كان تاليًا، وأعتقد أنه في الغالب كانت القرية هي الأسبق في الوجود.

٢) المطار التركي

حادثة أخرى حدثت في عام ١٩٩٧م في تركيا، ففي المطار الدولي لمدينة "استنبول" كان أحد مدارج المطار ينتهي عند سور المطار، وخارج السور مباشرة بعد انتهاء المدرج توجد إحدى الأسواق. وعادة تزدحم هذه السوق بمرتاديها وبالبائعين فيها طوال ساعات النهار وشطرًا كبيرًا من الليل. وحدث في يوم اشتد فيه هطول الأمطار أن هبطت الطائرة المصرية القادمة من القاهرة إلى استنبول في المطار الدولي للمدينة، وتم توجيهها إلى هذا المدرج، واستمرت الطائرة تدرج على أرض المدرج وساعدت سرعة الرياح في ذلك اليوم على ألا تتمكن الطائرة من تقليل سرعتها، بالإضافة إلى انزلاق عجلاتها على أرضية الممر (الملساء)! فكانت النتيجة أن الطائرة أكملت مشوارها حتى نهاية المدرج ثم حطمت سور المطار واقتحمت السوق. وكانت الخسائر المادية والبشرية كبيرة. هنا مرة أخرى يثور السؤال: من المسئول عن هذه الكارثة؟! إما اختيار السوق أو اختيار مدرج المطار.

٣) الطائرة السودانية

لم يمض زمن قليل على حادثة الطائرة المصرية حتى وقع حادث مؤسف لطائرة عسكرية سودانية كانت تقل عدداً من كبار ضباط الجيش السوداني في رحلة داخلية. وعند هبوط الطائرة كان هبوطها في ممر يقع على شاطئ البحر، وكان هذا الممر (عموديًا على الشاطئ وليس موازيًا له!)، وساعدت الرياح الشديدة التي كانت تهب بشدة على أن تندفع الطائرة وتستمر حتى نهاية المدرج ومن ثم تسقط في البحر. وكانت كارثة راح ضحيتها عدد من كبار ضباط الجيش السوداني.

ولا نخطئ السؤال هذه المرة فمن المؤكد أن اختيار اتجاه مدرج المطار هو الاختيار الخاطئ لأن مدرج المطار هو الذي تم بناؤه عموديًا على البحر وليس العكس!

٤) احتراق المجمع التجاري بمصر الجديدة

في صيف عام ١٩٩٦م فوجئ سكان مصر الجديدة (إحدى ضواحي مدينة القاهرة) بحريق هائل يشب في أحد المجمعات التجارية الضخمة (مول). وكان هذا المجمع التجاري مكونًا من أكثر من عشرة طوابق، وتحتل دار للسينما أحد الطوابق العليا منه. حدث الحريق في الساعة الثامنة مساء أحد الأيام التي ازدحم فيها المتسوقون ورواد دار السينما. كان سبب الحريق ماس كهربي في أحد أجهزة التكييف نتيجة زيادة الأحمال فاشتعل المكيف وبدأت النيران في الانتشار وصاحبها انقطاع الكهرباء الخاصة بالمبنى، مما أدى إلى تعذر الرؤية. وصاحب ذلك كله الدخان الكثيف الذي انبعث من احتراق المواد التي صنعت منها حوائط وأرضيات المبنى وبعض المواد المخزنة فيه، ونتج عن ذلك الدخان انعدام كامل للرؤية وإصابة الكثيرين بالاختناق.

تدافع الجمهور الكثير الذي كان متواجدًا في المجمع التجاري إلى سلالم الحريق في ظلام دامس للهروب من النار والدخان. وذكر بعض الشهود أن بعض أصحاب المحلات وضع بعضًا من صناديق البضائع على سلم الحريق في أحد الأدوار السفلية تمهيدًا لنقلها إلى مخازنهم، فاصطدم

الفارون من رواد المجمع بهذه الصناديق وعطلت هروبهم. ونتج عن ذلك تدافع من كانوا خلفهم ليصطدموا بهم ويقع من هرب من خطر الحريق فريسة للدهس بأقدام الفارين المذعورين.

الحادثة يجدها المتأمل مليئة بالدروس المستفادة بدءاً من اختيار موقع الأماكن المزدحمة بالجمهور، كالسينما، في الأدوار العليا وانتهاء بشغل سلالم الحريق بأشياء تعوق تحقيق الهدف الرئيسي من وجودها، مروراً بالمواد القابلة للاشتعال المصنوعة منها حوائط المبنى وأرضياته، وعدم وجود وسائل إضاءة احتياطية لاستخدامها عند انقطاع الكهرباء.

٢- أمن غرفة تشغيل الحاسب

يجب مراعاة الأمور التالية فيما يخص غرفة تشغيل الحاسب:

١) يجب أن تبقى غرفة الحاسب الآلي مغلقةً دائمًا، ويمنع الدخول إليها إلا لدواعي العمل.

٢) ضرورة تأمين النوافذ القريبة من الأرض، وأي فتحات أخرى موجودة بغرفة الحاسب.

٣) يجب تأمين المداخل والمخارج مع وجود أجهزة إنذار على الأبواب والنوافذ.

٤) تأمين جميع الكوابل وعزلها.

٥) وجود وسائل تصريف المياه في الأرضية (ربما احتاج الأمر إلى مضخات شفط المياه).

٦) إذا تطلب الأمر إخلاء المبنى فجأة، فيجب التأكد من إقفال غرفة الحاسب الآلي جيدًا، وتشغيل أجهزة الإنذار، كما يجب تدريب الموظفين على عملية الإخلاء الاضطرارية.

٧) وجود وسيلة مراقبة لما بعد ساعات الدوام، مع وجود الإجراءات الأمنية الملائمة، فيمكن عند الحاجة استخدام الدوائر التليفزيونية المغلقة، أو وسائل الإنذار الإلكترونية الحديثة.

٣- أمن الأجهزة

٣-١- تأمين الأجهزة داخل غرفة الحاسب

الإجراءات التالية لابد من اتباعها لضمان سلامة الأجهزة الموجودة داخل غرفة تشغيل الحاسب:

١) يجب أن يخضع دخول وخروج الأجهزة لموافقة مكتوبة من مسئول أمن نظام المعلومات.

٢) يجب تأمين الخدمات التي قد يسبب توقفها تلفاً بالأجهزة، مثل الطاقة الكهربية وتكييف الهواء.

٣) ضرورة وجود إجراءات معروفة ومعلنة تتبع عند الطوارئ لفصل التيار الكهربائي ويجب التدريب على تنفيذها من آنٍ لآخر.

٤) لا يجب أن يسمح لمسئولي الصيانة من خارج المؤسسة بإدخال أو نزع البطاقات الإلكترونية، مثل: بطاقات الدوائر المتكاملة دون الموافقة المسبقة لمسئول أمن أنظمة المعلومات.

٥) ضرورة مرافقة مسئولي الصيانة من خارج المؤسسة خلال عملهم لعدم وضع أجهزة تنصت أو ما أشبه.

٦) وضع إجراءات يلزم اتباعها عند إخراج الأجهزة للصيانة خارج المبنى، وعند إعادتها.

٣-٢- تأمين النهايات الطرفية والطابعات

لأن المعلومات الآن يمكن الوصول إليها عن بعد من خلال "الطرفيات" التي قد تكون موجودة في مكان بعيد، أو ربما في دولة أخرى، فإن الأمر يتطلب إجراءات معينة يمكن إيجازها فيما يلي:

١) متابعة سجل الأعمال (LOG) باستمرار لمتابعة عمليات دخول المستفيدين إلى النظام واستخدام المعلومات.

٢) تقييد استخدام البرامج الخاصة بنقل البيانات بين الحاسبات الشخصية والحاسب الكبير، لأن ذلك يمثل وسيلة سهلة لتسريب البرمجيات وغيرها من المعلومات.

٣) مراقبة أماكن الطباعة التي يتم فيها إخراج النسخ المطبوعة لتقليل فرصة حصول غير المرخص لهم على قوائم أو بيانات مطبوعة لا يجب إطلاعهم عليها.

٤) ضرورة وجود مفاتيح لإغلاق الطرفيات، أو الغرف الموجودة بها، عند عدم استخدامها.

٥) ضرورة ربط تصريح الاستخدام بالطرفية الموجودة في منطقة عمل الموظف.

٦) ضرورة التأكد من فصل الطرفيات والطابعات خارج ساعات الدوام.

٧) ضرورة وجود قوائم يتم تحديثها أولاً بأول لجميع الطرفيات ومستخدميها وأماكن وجودها، ويفضل وجود نظام آلي لمتابعتها.

٣-٣- المواقع البديلة

تهتم الجهات التي تعتبر تعطل الحاسب فيها أمرًا غير مقبول بأن يكون هناك مكان بديل يتم استخدامه في حالة تعذر استخدام الحاسب الأصلي سواء بسبب تدمير المبنى أو بسبب تعطل الجهاز، ومن أمثال هذه الجهات: شركات الطيران والقوات المسلحة ، وسوف نتعرض لهذا الموضوع بتفصيل أكثر لاحقًا.

٤- أمن وسائط المعلومات

إذا كانت المعلومات هي الكنز الثمين الذي يجب على المؤسسة الحفاظ عليه، فإن الوسائط التي تستخدم لتخزين المعلومات يجب أن تحصل بدورها على القسط الوافر من الاهتمام. ولذلك يجب اتخاذ الاحتياطات التالية لتأمين مكتبات تخزين البيانات:

١) ينبغي توفير مستوى حماية مناسب للأسطوانات والأشرطة الممغنطة والأقراص الضوئية التي تحتوي على المعلومات، بحيث يكون على نفس مستوى الحماية المتاح لأجهزة الحاسب الآلي.

٢) يجب أن يتم الاحتفاظ بالوسائط التي تحتوي على النسخ الاحتياطية من الملفات في مكان بعيد عن الموقع حتى لا تتعرض للتلف عند حدوث كارثة للموقع لا قدر الله، وأن يتم التخزين في خزائن مغلقة بإحكام، ويجب أن تكون هذه الخزائن مقاومة ضد الحريق والماء والزلازل.

٣) ينبغي أن يقتصر الوصول إلى مناطق تخزين هذه الوسائط على الأشخاص المصرح لهم فقط دون غيرهم.

٤) ينبغي الاهتمام بإتلاف النفايات والمخلفات مثل البطاقات وقوائم البرامج والميكروفيلم باستخدام أفران حرق الأوراق وآلات خرط الورق وغيرها، أما بالنسبة لوسائط تخزين المعلومات الممغنطة من أسطوانات وأشرطة والتي انتهت الحاجة إليها فيجب إزالة مغنطتها قبل التخلص منها.

٥) الحذر عند استخدام بعض الأجهزة الإلكترونية بقرب وسائط المعلومات، خاصة تلك التي تحتوي على مغناطيس أو ملفات كهربية أو أجهزة ينشأ عنها مجال مغناطيسي، وذلك لاحتمال تأثيرها على البيانات المسجلة.

٦) ضرورة تخزين الوسائط القابلة للتفكيك والحمل، مثل الأسطوانات المرنة والأشرطة، في نهاية كل يوم داخل غرفة مغلقة، كما يجب أن تكون هناك إجراءات ودفاتر تنظم تداولها.

٥- أمن الأفراد

لعل **الأفراد من أثمن ما تمتلكه المؤسسات**، وهم قد يكونون في الوقت نفسه من بين الأخطار الحقيقية التي قد تهدد أمن النظام! ولذلك يجب الاهتمام بالتوصيات التالية من أجل المحافظة على أمنهم وضمان التزامهم بالأمن:

١) تنظيم ومتابعة تسجيل دخول الموظفين وخروجهم من المبنى وتنقلهم داخله.

٢) تنظيم دخول الزائرين ومرافقتهم داخل المبنى، وضرورة وجود سجل للزوار ومتابعة وجودهم بالمبنى.

٣) مراقبة اتصال المستفيدين من الخارج ومتابعة استخدامهم للنظام.

٤) متابعة سجل عمليات المستفيدين، وخاصة هؤلاء الذين لديهم صلاحيات عالية لاستخدام البيانات.

٥) اشتراط تحديث كلمات السر أولاً بأول.

٦) تحديد الإجراءات المتبعة في حالة الاستقالة أو إنهاء الخدمة أو تغيير مجال العمل، ويجب أن تتضمن هذه الإجراءات شطب الموظف الذي انتهت خدمته من قائمة المسموح لهم باستخدام النظام، وكذلك تغيير كلمات السر (ربما لمجموعة كاملة من الموظفين في حالة اطلاع الموظف الذي انتهت خدمته على هذه المعلومات بحكم عمله).

٧) اختيار الموظفين بعناية، وإجراء التحريات اللازمة عنهم خصوصًا بالنسبة للأجانب الذين يتولون مراكز حساسة تكون لها صلاحيات عالية لاستخدام المعلومات.

٨) لا يجب أن يحصل الموظف حديث التعيين على صلاحيات عالية لاستخدام النظام.

٩) ضرورة وجود قائمة، أو نظام آلي، لدى مسئول أمن نظام المعلومات تضم كافة الأشخاص المصرح لهم باستخدام النظام ودرجات صلاحياتهم.

١٠) ضرورة حصول كل مستخدمي النظام على تدريب مناسب حول الأمن يتضمن نقاط الضعف والأخطار التي تهدد النظام والإجراءات المضادة اللازمة.

١١) يجب أن تتضمن عقود التوظيف شرطاً يمنع الموظفين من إفشاء المعلومات الحساسة أو إفشاء إجراءات الأمن والرقابة.

٦- دور ضابط أمن نظم المعلومات

تتمتع وظيفة ضابط أمن نظم المعلومات بأهمية قصوى، ويجب أن يتولى هذا الضابط الإشراف على جميع إجراءات الأمن في المؤسسة، وتكون مهامه:

١) اقتراح وتطبيق السياسة الأمنية لنظم المعلومات.

٢) تأمين مركز الحاسب وشبكة الاتصالات والطرفيات.

٣) الاتصال باستمرار مع مستخدمي الحاسب.

٤) إعداد معايير وإجراءات الأمن والسلامة والتأكد من تطبيقها.

٥) تحليل الأخطار المتوقعة ومراقبتها.

٦) اقتراح وتطبيق الوسائل الفنية اللازمة لتنظيم ومراقبة استخدام المستفيدين للحاسب سواء كانت هذه الوسائل من الأجهزة (Hardware) أو البرمجيات (Software).

٧) وضع خطة الطوارئ (Contingency plan) والإشراف على اختبارها وتطويرها وتنفيذها.



الفصل الثالث

جرائم الحاسب

موضوعات الفصل:

(١) الاستخدامات غير المشروعة للحاسبات.

(٢) أنواع جرائم الحاسب.

(٣) أمثلة على جرائم الحاسب في العصر الحديث.

(٤) أساليب مكافحة جرائم الحاسب.

(٥) التشريعات في مجال مكافحة جريمة الحاسب.



استهللنا هذا الفصل الذي خصصناه للحديث عن جرائم الحاسب بتحديد الاستخدامات غير المشروعة للحاسبات، ثم محاولة تصنيف أنواع جرائم الحاسب، ثم قدمنا بعض الأمثلة على أنواع جرائم الحاسب المختلفة في العصر الحديث. انتقلنا بعد ذلك إلى الحديث عن أساليب مكافحة جرائم الحاسب واستخدام التقنية الحديثة في ذلك، وما هي الاحتياجات الأمنية العربية في هذا المجال. خصصنا بعد ذلك قسمًا هامًا للحديث عن التشريعات في مجال مكافحة جريمة الحاسب، واختلاف التشريعات من بلد إلى آخر وكيف أن هذه المشكلة يجب حلها بعد دخولنا لعصر الإنترنت وسهولة وحرية انتقال المعلومة من بلد إلى آخر، وفي هذا الصدد أوردنا محاولات الدول الأوروبية لتوحيد تشريعاتها ومدى نجاحها في ذلك.

١- الاستخدامات غير المشروعة للحاسبات

يندرج ما يحدث من تزوير أو اختلاس أو إتلاف للبيانات تحت مسمى **الاستخدامات غير المشروعة للحاسبات**، وكانت البنوك مثلاً، في أحوال متعددة، عرضة لبعض حالات الاختلاس والتلاعب بحسابات العملاء، بل إن بعض الشبكات الحيوية في بعض الدول المتقدمة كانت عرضة للاختراق أكثر من مرة، بل ومن جانب غير المحترفين.

ويمكن تقسيم الوسائل غير المشروعة في استخدام الحاسب الآلي إلى:

١) تزوير البيانات عند إدخالها إلى الحاسب.
٢) تغيير برامج الحاسب أو إعداد برامج خصيصاً بهدف التلاعب.
٣) سرقة المعلومات والخطط من مؤسسة واستخدامها لأغراض مؤسسة منافسة.
٤) استخدام وقت الحاسب في غير أغراض المؤسسة.
٥) سرقة برامج الحاسب نفسها.

٢- أنواع جرائم الحاسب

من الصعب أن نحاول حصر أنواع جرائم الحاسب فهذا الحصر يختلف من مجتمع لآخر، وربما يتحدد بدرجة نضج المجتمع ودرجة استخدامه للحاسب الآلي واعتماده عليه. ولكن لنرى كيف صنف المجلس الأوروبي أنواع جرائم الحاسب الآلي، فقد اقترح على الدول الأعضاء فيه أن تضع قوانينها الجنائية في الاعتبار ثمانية أنواع من الأنشطة المتعلقة بالحاسب الآلي والتي يجب تجريمها [Carr 1994]. وتضم هذه الأنشطة قائمة إجبارية، وتشمل هذه القائمة:

١) الاحتيال باستخدام الحاسب.
٢) التزوير باستخدام الحاسب.
٣) تدمير بيانات أو برامج الحاسب.
٤) تخريب الحاسب.
٥) الوصول للبيانات بدون تصريح.
٦) اعتراض مسار البيانات المنقولة بدون تصريح.
٧) إعادة إنتاج برامج الحاسب المحمية بدون تصريح.
٨) إعادة إنتاج الخرائط والرسوم بدون تصريح.

كما اقترح المجلس الأوروبي على أعضائه أربعة أنشطة تتضمنها قائمة أخرى (اختيارية)، ولكنه ترك للدول الأعضاء حرية التصرف في أسلوب التجريم والعقوبة بالنسبة لجرائم هذه القائمة الاختيارية وهي تتضمن:

٩) تعديل برامج الحاسب الآلي أو بياناته.
١٠) التجسس على أنشطة الحاسب.
١١) استخدام الحاسب بدون تصريح.
١٢) استخدام برامج الحاسب المحمية بدون تصريح.

وقد استجابت معظم الدول الأعضاء لهذه التوصيات [Carr 1994]. ويتضح من الحصر السابق أن جريمة مثل حذف بيانات الحاسب لم يتم تجريمها من قبل الاتحاد الأوروبي سواء في القائمة الإجبارية أو الاختيارية، حيث الحذف لا يعتبر تدميرًا أو تزويرًا أو تخريبًا وفقًا لتعريف القانون البريطاني والاسكتلندي كما سنوضح لاحقًا. ونقترح هنا أن تضاف هذه الجريمة بوضوح إلى القائمة ، وقبل ذلك نقترح أن تأخذ هذه القائمة حقها من الدراسة في مؤسساتنا التشريعية العربية حتى نستطيع التصدي لنوع جديد من الجرائم يطلق عليه اسم "جريمة العصر" حيث لا يوجد فيها آثار أقدام أو قفل مكسور أو بصمات أصابع ، بل إن الضحية قد لا يعرف بوقوع الجريمة وهذا أخطر ما في الأمر.

٣- أمثلة على جرائم الحاسب في العصر الحديث

يذكر التاريخ الحديث للحاسب عدة جرائم كان من أشهرها:

١) في يوليو ١٩٨٩م نشرت الصحف اللندنية أن اثنين من المبرمجين في إحدى المؤسسات الحكومية المهمة قد تم طردهما لأنهما تسببا في تعطيل شبكة الحاسبات الخاصة بالمؤسسة خلال إضراب قام به أعضاء النقابة التابعين لها، وقد تم تعطيل الشبكة لمدة يوم كامل مما تسبب في منع الموظفين الآخرين بالمؤسسة من أداء أعمالهم. وقد استخدم هذان المبرمجان صلاحياتهما الخاصة لإدخال التعليمات التي تسببت في تعطيل نظام معالجة الكلمات الذي يخدم ثلاثة حاسبات متوسطة تضمها الشبكة والتي تصل ٢٤ نهاية طرفية. فضلاً عن ذلك، فقد قاما بنزع وإخفاء مفاتيح تشغيل الحاسبات. وقد اضطرت المؤسسة إلى استدعاء مهندسي شركة الحاسبات لتغيير هذه المفاتيح وتصحيح البرامج وإعادة تشغيل النظام.

٢) في إضراب آخر في الولايات المتحدة، والذي دام أربعة أشهر في عام ١٩٨٩م، وشمل مهندسي الاتصالات، تم اكتشاف سلوك إجرامي من جانب بعض المضربين المتطرفين، فقد تم تخريب صناديق التوصيل التي تحتوي على وصلات خطوط نقل الصوت والمعلومات، كما تم ضبط أكثر من (٧٠٠) حادث قطع لخطوط الهاتف بغرض عرقلة الاتصالات الهاتفية وعمليات نقل البيانات، وفي إحدى هذه الحوادث تم قطع خطين رئيسيين من خطوط الألياف البصرية التي تشكل العامود الفقري لشبكة الاتصالات في مركز الاتصالات الرئيسي بالمدينة، مما نتج عنه تعطل حوالي ٢٠٠,٠٠٠ خط هاتفي لمدة ٢٤ ساعة.

٣) في حادث آخر وقع في الولايات المتحدة قام بعض المخربين -بهدف تشويه سمعة شركة الاتصالات الهاتفية- بتدمير أطباق استقبال الاتصالات الخاصة بالمستفيدين (سواء الميكروويف أو الأقمار الاصطناعية)، كما قاموا بالاتصال ببعض الأرقام الهاتفية الحيوية لشغل الخط وتعطيل الخدمة، بل إنهم قاموا كذلك بالدخول إلى نظام الخدمة الهاتفية الآلي ، باستخدام بعض كلمات السر ذات الصلاحيات العالية التي سمحت لهم بتجاوز الاحتياطات الأمنية المختلفة، ومن ثم تغيير البرامج وتبديل أرقام المشتركين في جداول الخدمة مما سبب اضطراباً هائلاً في الخدمة الهاتفية.

٤) حدثت الواقعة التالية خلال حرب فيتنام في أواخر الستينيات من القرن الماضي في إحدى شركات الكيماويات الكبرى في الولايات المتحدة التي قامت بتصنيع إحدى المواد الكيميائية (Orange agent) التي كانت الطائرات الأمريكية تقوم برشها فوق الغابات لإبادة أوراق الأشجار حتى لا يتمكن الفيتناميون من الاختفاء بينها، وقد تسببت هذه المادة في الكثير من المشكلات الصحية الخطيرة للجنود الأمريكيين أنفسهم. وخلال إحدى

المظاهرات المعارضة للحرب تم احتلال مركز المعلومات الرئيسي لهذه الشركة بواسطة المتظاهرين الذين دام احتلالهم للمبنى ثلاثة أيام حتى غادروه بسلام. وقد كانت سعادة موظفي الشركة كبيرة عندما بدا أن المتظاهرين لم يتمكنوا من تخريب نظام الحاسب، وعزوا ذلك لعدم معرفتهم بكيفية تنفيذ ذلك. ولكن عندما حاول الموظفون إعادة تشغيل الحاسب كانت المفاجأة، ففي مكتبة الشرائط التي كانت تحتوي على سبعة آلاف شريط ممغنط مستخدمة لتخزين ملفات الشركة المهمة والملفات الاحتياطية، تم إخراج كل شريط من حاويته ووضعه في حاوية أخرى لشريط آخر. ولمَّا كانت عناوين الأشرطة مسجلة على الحاويات فقط وليس على الأشرطة نفسها؛ فيمكن تخيل مدى الفوضى التي حلت بمكتبة الشرائط مما اضطر الموظفين إلى قراءة كل شريط باستخدام الحاسب لتحديد هويته الحقيقية، وخلال عملية طويلة وشاقة استغرقت أسبوعًا كاملاً تم إعادة "التزاوج" بين الأشرطة وحاوياتها، وأمكن بعد ذلك فقط إعادة تشغيل النظام.

٥) تعرض أحد البنوك الرئيسية في مدينة بوسطن بالولايات المتحدة لعدة حوادث سرقة استهدفت الحاسبات الشخصية دون غيرها من مبنى المركز الرئيسي، وخلال التحقيقات التي تمت في هذه الحوادث اكتشف البنك خللاً كبيرًا في نظام الأمن فيه: لمَّا كان على جميع الزوار أن يوقعوا عند دخولهم المبنى في دفتر مخصص لذلك، فقد كان موقع حارس الأمن عند منطقة الاستقبال بالدور الأرضي، وكان للمبنى الرئيسي للبنك قبو لمواقف السيارات محجوز بالكامل لموظفي البنك، وكان الوصول إلى منطقة المواقف، ومن ثم إلى باقي أدوار المبنى، محكومًا عن طريق استخدام بطاقة ممغنطة يحملها جميع موظفي البنك ليمكنهم استخدام المواقف ومن ثم الوصول إلى مكاتبهم. وتبين أن تسرب

الأجهزة تم بواسطة أحد الموظفين عن طريق استخدام مصاعد البنك لنقل الأجهزة إلى القبو ومن ثم إلى سيارته ثم الخروج من القبو ببساطة، وفي أعقاب هذا الحادث قام البنك بتركيب كاميرات تليفزيونية في القبو لمراقبة المصاعد.

٦) تعاقدت إحدى شركات قطع الغيار مع مبرمج متعاون لتطوير نظام لمتابعة المخزون بمخازن الشركة، وعقب انتهاء العمل ترك المبرمج الشركة، وبعد فترة اتصل بالشركة أحد تجار قطع الغيار بشأن نظام لمتابعة المخزون تم عرضه للبيع إليه بواسطة أحد المبرمجين، وعند اختبار النظام وجد التاجر اسم شركة قطع الغيار على بعض مخرجات النظام فشك في الأمر. الواضح في هذه الواقعة أن المبرمج حاول بيع النظام مرة أخرى لهذا التاجر. وعندما حاولت الشركة مقاضاة المبرمج نصحها مستشارها القانوني بالنكوص عن ذلك لأن الرجل يعمل بمفرده وحتى في حالة صدور حكم قضائي لصالح الشركة فلن تستطيع الحصول منه على أي تعويض.

٤- أساليب مكافحة جرائم الحاسب

٤-١- استخدام التقنية

١) التقنية في خدمة صناعة الأمن

التقدم المستمر في التقنية يبدو بغير حدود، ذلك التقدم تتم الاستفادة منه في صناعة الأمن للمساعدة في مكافحة الجريمة ومكافحة الإرهاب، ولذلك أخذت صناعة الأمن في النمو بسرعة ملحوظة في السنوات الأخيرة، وسنتعرض في معرض حديثنا عن أساليب مكافحة جرائم الحاسب للتطورات التقنية التي طرأت مؤخرًا على أسواق المعدات الأمنية التي تُخرج لنا في كل

يوم جهازًا جديدًا أو فكرة جديدة تساعد خبراء الأمن في مجال مكافحة الجريمة، وسنقصر عرضنا على المعدات التقنية الحديثة التي تستخدم للتأمين المادي للمباني والمناطق المكشوفة .

٢) التقنية الحائرة بين فرض القانون وخرقه

في الوقت الذي نرى فيه التقنية الحديثة تطوع نفسها لخدمة أغراض الأمن ومكافحة الجريمة، فإن أولئك الذين يقومون بتحدي المؤسسات التي تحمل على عاتقها مسئولية فرض سيادة القانون لم يتوانوا بدورهم عن اقتناء هذه التقنيات المتقدمة والاستفادة منها للوصول إلى أهدافهم. ومن المؤكد أن التهديد الناشئ عن العمليات الإرهابية التي تقع في أماكن كثيرة من العالم قد فرض إنتاج وتطوير وسائل وأساليب وتقنيات جديدة للتصدي لأعمال العنف، فنرى الكثير من الشركات النشطة في مجال المراقبة وقد حولت اهتمامها إلى الأسواق الأمنية المتعطشة للوسائل الحديثة لمراقبة المباني والمناطق المكشوفة التي تكون لها طبيعة هامة وحساسة.

٣) التقنية في منطقة الشرق الأوسط

في دول العالم المختلفة تنمو سوق المعدات والأجهزة الأمنية بشكل متواصل، أما في دول الشرق الأوسط فيتوقف هذا النمو على عدة عوامل منها درجة الإحساس بالخطر وحدة التوترات الإقليمية أو الاضطرابات الداخلية في بلدان المنطقة. والسوق العربية لا تقل اهتمامًا بتقنيات مكافحة الجريمة عن غيرها من أسواق المنطقة، فقد بدأ الكثير من أجهزة الشرطة في الدول العربية بالأخذ بالتقنية سواء في إصدار بطاقات الهوية الحديثة أو في أساليب المراقبة أو حتى في مجالات اقتفاء الأثر للمساعدة في القبض على المجرمين، ولكن تأتي دائمًا الميزانيات المالية المحدودة لتقف عائقًا خطيرًا يحول دون اقتناء التقنيات الحديثة في هذه الدول.

٤) أمن المطارات أهدى التقنية إلى المجالات الأخرى

ومن الإنصاف أن نذكر أن كثيرًا من التقنيات الأمنية التي تشهدها الأسواق هذه الأيام جاءت نتيجة الحاجة إلى حماية حركة النقل الجوي للركاب والبضائع من الإرهاب والحاجة الماسة إلى تطوير أساليب مكافحة تهريب المخدرات عبر المطارات، وقد ازدادت أهمية هذا الموضوع بشكل ملحوظ في أعقاب موجة خطف الطائرات التي عانت منها مطارات العالم في حقبة السبعينيات من القرن العشرين وما بعدها. وقد شجعت هذه الحاجة المتزايدة والملحة على ابتكار العديد من التطورات التقنية الهامة التي أنتجتها الشركات المتخصصة بناء على توصيات منظمة الطيران المدني العالمية التي قامت بإعداد مواصفات محددة ودقيقة في مجال أمن المطارات والطائرات والركاب التزمت بها جميع مطارات العالم.

٤-٢- الاحتياجات الأمنية العربية

مما تقدم يتضح أن الاحتياجات الأمنية بطبيعتها متعددة ومتنوعة وتكاد تكون غير محدودة، وهي بالإضافة إلى كل ذلك حقل متغير باستمرار، فهي تلاحق التقنية بشكل مستمر كما تلاحق المجرمين لاستخدام الأحدث والأفضل في مكافحة الجرائم، وهذا النطاق الواسع المتغير يقوم بتغطيته العديد من الشركات المتخصصة في الشئون الأمنية. ولعل السوق العربية في أمس الحاجة لزيادة الوعي بالأمن والاهتمام به، وما مر مؤخرًا بمنطقتنا من أحداث يدفعنا إلى أن نولي هذه الأمور الأمنية عناية خاصة وبالذات في ظل التطور المستمر للتقنية.

٥- التشريعات في مجال مكافحة جرائم الحاسب

٥-١- حماية البيانات الشخصية المتداولة

٥-١-١- أهمية تداول البيانات الشخصية

من المؤكد أن البيانات تُستخدم حاليًا، وسوف تُستخدم في المستقبل على نطاق أوسع ، في القطاع التجاري بالذات من أجل تبادل المعلومات بين جهات مختلفة، سواء داخل الدولة الواحدة أو على مستوى العالم. هذه المعلومات منها مواصفات المنتجات وأسعارها، وغير ذلك. من المتوقع على أي حال أن يكون لتداول البيانات وتبادل المعلومات دور رئيسي في قطاعات، مثل: التأمين والبنوك بالإضافة إلى القطاعات الحكومية الأخرى، مثل: الخدمات الصحية والاجتماعية والجمارك والجوازات والشرطة وغيرها من المجالات. معنى ذلك أنه بالإضافة إلى المعلومات التجارية فهناك الكثير من المعلومات الشخصية عن الأفراد يتم تداولها من خلال شبكات المعلومات، وهذا التداول مهم ومطلوب ومفيد للمجتمع بل وللفرد نفسه، ومن الطبيعي أن يكون لهذه المعلومات خصوصية يجب الحفاظ عليها. فما هي التشريعات التي تحمي خصوصية المعلومات الشخصية عن الأفراد؟

٥-١-٢- الخصوصية الفردية في العالم المتقدم

في أوروبا تعترف دول الاتحاد الأوروبي بحق الخصوصية كمبدأ (باستثناء بلجيكا واليونان وإيطاليا وأسبانيا التي لم نتمكن من التأكد إذا كان لديها تشريعات لحماية الخصوصية الفردية) وتقوم الدول التي تعترف بحق الخصوصية بسن التشريعات التي توفر حماية واضحة للبيانات الشخصية للأفراد، خاصة عندما يتم تخزينها على الحاسب الآلي، وذلك بمنع استخدامها

سواء داخل الدولة العضو في الاتحاد أو إذا تم نقلها إلى دول أخرى. وهذه التشريعات تختلف من دولة لأخرى وفقًا لنوع وطبيعة المعلومات التي تحميها كما تختلف من حيث الوسائل التي تتم من خلالها هذه الحماية. كان الدافع الرئيسي لاهتمام بعض الدول الأعضاء هو الإيمان بالخصوصية الفردية، بينما كان دافع البعض الآخر هو الرغبة الشديدة في التناغم مع الدول الأخرى الأعضاء، إذ كان ذلك أحد شروط الانضمام إلى الاتحاد. لذلك نجد أن الدول الأعضاء تختلف في درجات حمايتها للخصوصية الفردية فبعضها يحمي المعلومات الشخصية المخزنة على الحاسب والخاصة بالأفراد الأحياء فقط، والبعض الآخر (الدانمارك والنمسا) يمد مظلة هذه الحماية إلى الشخصيات الاعتبارية، مثل: الشركات والنقابات وغيرها، بينما نرى دولاً أخرى (فرنسا وألمانيا وهولندا) تمد مظلة الحماية إلى أبعد مدى فتحمي البيانات الورقية وبيانات الحاسب وجميع أنواع البيانات الشخصية أيًا كان الوسط الذي تقع عليه [Carr 1994].

في بعض البلاد خارج نطاق الاتحاد الأوروبي تقتصر حماية البيانات على حالة استخدامها بشكل علني (الولايات المتحدة ونيوزيلندة) ، وواضح أن الهدف هنا هو حماية الفرد من التشهير فقط.

٥-١-٣- الخصوصية الفردية في العالم الثالث

أما دول العالم الثالث (أمريكا اللاتينية وأفريقيا) فقد اقترحت أن الحماية يجب أن تشمل المعلومات التي تمس السيادة الوطنية أو الرخاء الاقتصادي أو المصالح الثقافية والاجتماعية للشعوب. ويتضح هنا أن الحظر هو في الحقيقة لصالح الدولة أو مجموع الشعب وليس لصالح الأفراد، وهو يتخذ غطاء لحماية الحكومات. فعندما أصدرت حكومة جمهورية مصر العربية تشريعًا (نشر بجريدة الوقائع المصرية عام ١٩٨٦م) يقضي بسرية

بيانات الأرصدة في البنوك وعدم جواز إفشائها حتى للإدارات الحكومية، لم يطلق المشرع هذا الحكم بلا استثناء ولكنه استثنى الحالات التي يصدر بها أمر من النيابة العامة وفرض على البنوك الامتثال لمثل هذه الأوامر. بينما نرى الحكومة السويسرية والبنوك جميعها في الاتحاد السويسري تمنح حماية كاملة وسرية لا استثناء فيها على أرصدة العملاء وحساباتهم وحركة هذه الحسابات. ومن المفهوم أن الدافع وراء هذا الاتجاه هو دافع اقتصادي بحت.

٥-٢- اختلاف القوانين

٥-٢-١- أثر ظهور شبكة إنترنت

بعض الدول التي تضع قيوداً على تداول المعلومات تطلب، في حالة انتقال هذه المعلومات إلى دولة أخرى، أن تلتزم هذه الدولة بنفس مستوى الحماية المفروض على هذه المعلومات، وربما كان هذا من حق الدولة ولكن امتداد القيود عبر الدول مع اختلاف قوانين الدول عن بعضها يسبب مشاكل كثيرة لرجال الأعمال الذين يحتاجون إلى تبادل المعلومات عبر العالم وخاصة بعد ظهور شبكة الإنترنت. وفي الحقيقة فإن ظهور الإنترنت أنشأ أمرًا واقعًا لا تستطيع الدول أن تفعل شيئًا في مواجهته. هذا الأمر الواقع هو صعوبة ملاحقة المعلومات. فأنت تستطيع التحكم في أنبوب ينقل الماء من مكان إلى آخر وأن تراقب ما ينقله هذا الأنبوب ، ولكنك لا تستطيع بأي حال من الأحوال أن تراقب الطوفان إذا زحف وأغرق واجتاح.

٥-٢-٢- درجة الحماية بين القانون البريطاني ونظيره الألماني

ولكي نبين اختلاف القوانين بين الدول نذكر أن القانون البريطاني مثلاً كل ما يفرضه على مستخدم المعلومة أن يسجل استخدامه لها ولا يشترط

حصوله على ترخيص بذلك، بينما القانون الألماني يشترط حصول مستخدم المعلومة على تصريح بذلك. فالقانون البريطاني إذن يمنح درجة من الحماية أقل من تلك التي يمنحها القانون الألماني [Hoeren 1994].

٥-٣- محاولات توحيد التشريعات

احتاج الاتحاد الأوروبي خمسة عشر عامًا من المناقشات والمداولات حتى انتهى إلى وضع مسودة إعلان النوايا التي مهدت الطريق لإصدار تشريع لتداول المعلومات، وقد تم التوصل لهذه المسودة في عام ١٩٩٠م وتمت موافقة البرلمان الأوروبي على نسختها المعدلة في عام ١٩٩٢م [Official Journal 1992]. في هذا الإعلان تم ولأول مرة حصر الحالات التي يكون فيها استخدام البيانات الشخصية قانونيًا ومباحًا وهي:

١) أن يوافق على ذلك صاحب البيانات.

٢) أن يكون استخدام البيانات ضروريًا لإبرام تعاقد مع صاحب البيانات أو من أجل البت في طلب مقدم من صاحب البيانات قبل التعاقد معه.

٣) أن يكون استخدام البيانات ضروريًا من أجل تنفيذ التزام يفرضه القانون الدولي أو قانون الاتحاد الأوروبي.

٤) أن يكون استخدام البيانات ضروريًا لحماية المصالح الحيوية لصاحب البيانات.

٥) أن يكون استخدام البيانات ضروريًا لأداء مهمة تخدم الصالح العام، أو مهمة تقوم بها سلطة عامة تكون مكلفة بذلك أو تكون ضرورية لطرف ثالث يلزم أن تُكشف له هذه البيانات.

٦) أن يكون استخدام البيانات ضروريًا للمحافظة على الصالح العام أو للحفاظ على المصالح المشروعة لطرف ثالث يلزم أن تُكشف له هذه البيانات، ما لم تتعارض هذه المصالح مع مصالح صاحب البيانات نفسه.

٥-٤- التشريع في مواجهة جرائم الحاسب

تزوير بيانات الحاسب هي جريمة أداتها استخدام طرفية ومسرح الجريمة فيها هو الحاسب الآلي نفسه، تمامًا كجريمة القتل التي قد تكون أداتها سلاحًا ناريًا أو سكينًا. وهذه الجريمة (التزوير) تكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها، إذ يُعرِّف القانون البريطاني التزوير بأنه "يعتبر الشخص مدانًا بالتزوير إذا اصطنع أداة زائفة بنية استخدامها، سواء بنفسه أو بواسطة آخرين، لإقناع شخص ما بقبول هذه الأداة باعتبارها أداة حقيقية، فيقبلها نتيجة لذلك للقيام، أو عدم القيام، بعمل ما ينتج عنه ضرر له أو لآخرين". هذه الأداة في مجال الحاسب قد تكون قرصًا ممغنطًا أو شريطًا أو أي وسط لحفظ البيانات. بينما ينص القانون الاسكتلندي على "الدخول غير المشروع إلى برنامج أو بيانات مخزنة على الحاسب، إذا تم ذلك بغرض الحصول على معلومات من البرنامج أو البيانات أو الإضافة إلى البرنامج أو البيانات أو الحذف من أي منهما أو التعديل في أي منهما، بنية حصول مرتكب الواقعة على ميزة لنفسه أو لغيره أو إلحاق الضرر بمصالح شخص آخر" [Collier 1994].

في بعض الأحوال تنتج عما نسميه جرائم الحاسب أضرار كبيرة (اقتصادية في الغالب)، ولكن الجرائم في هذه الحالة لا تقع في دائرة التجريم من جانب القانون الجنائي. فجرائم الحاسب لها خصوصية تجعل التشريع يقف عاجزًا عن تكييفها قانونيًا أو إخضاعها لمواد القانون الجنائي، من هذه الخصوصية أن جرائم الحاسب لا تقع على أرض دولة معينة بحيث يختص قضاء هذه الدولة بالنظر فيها، فقد يقوم شخص ما جالس أمام جهاز الحاسب الشخصي في دولة ما باستخدام نظام الحاسب في دولة أخرى ويقوم إما بالحصول على المعلومات أو تدميرها أو تزويرها، هذه السهولة في عبور النشاط الإجرامي للحدود يجب أن تجعلنا ننظر بشكل مختلف إلى جرائم الحاسب.

ونود أن ننبه هنا إلى أن جرائم الحاسب هي جرائم من نوع فريد وتحتاج إلى تشريعات خاصة ووسائل مختلفة للإثبات بل وتحتاج إلى شرطة خاصة لمكافحتها تكون مدربة بشكل خاص على هذا النوع من الجرائم. فبعض التشريعات تتطلب، كي تجرم الفعل، أن يكون هناك اقتحام أما بالنسبة للمعلومات فكيف نعرّف الاقتحام؟ هل تخمين كلمة السر واستخدامها في الدخول إلى قاعدة بيانات للحصول على معلومات يعتبر اقتحامًا؟ وهل يشترط أن يقوم الحاسب بتحذير المقتحم عند الدخول إلى البيانات بأن ذلك يضعه تحت طائلة القانون؟.

أعتقد أن هناك تعديلات كثيرة مطلوب إدخالها على التشريعات التي تتعامل مع الجريمة كي تأخذ في الاعتبار المعطيات الجديدة التي نشأت عن استخدام الحاسب الآلي في مجال المعلومات وعن ظهور شبكات المعلومات العالمية، وأعتقد أن هذا يمكن أن يكون نقطة بحث جديدة ندعو الباحثين للاهتمام بها.

الفصل الرابع

فيروسات الحاسب

موضوعات الفصل:

(١) ماهية الفيروسات ونشأتها.
(٢) أنواع الفيروسات.
(٣) طرق الوقاية من الفيروسات.
(٤) طرق علاج آثار الفيروسات.



نشر الفيروسات جريمة من جرائم الحاسب، بل هي من أخطر هذه الجرائم، ولذلك أفردنا لها هذا الفصل تاليًا لفصل جرائم الحاسب. وقد بدأنا هذا الفصل بالحديث عن ماهية الفيروسات وطبيعتها ونشأتها، وألقينا عليها نظرة من الداخل لمحاولة تقريب أسلوب عملها للقارئ العادي. أعقبنا ذلك بالحديث عن الأنواع المختلفة من الفيروسات، ثم تحدثنا عن طرق الوقاية منها، وعن الإجراءات التي يجب أن تتخذ في مواجهتها من جانب الفرد أو المنشأة أو إجراءات ذات طابع أشمل، ثم تحدثنا عن عيوب الرقابة الأمنية الصارمة وتقبل المستفيدين لها، ثم اختتمنا هذا الفصل بالحديث عن طرق علاج آثار الفيروسات إذا لم تفلح إجراءات الوقاية في درء شرها.

١- ماهية الفيروسات ونشأتها

١-١- ما هو الفيروس؟

الفيروس في حقيقته هو برنامج من برامج الحاسب ولكن تم تصميمه بهدف إلحاق الضرر بنظام الحاسب، وحتى يتحقق ذلك يلزم أن تكون لهذا البرنامج القدرة على ربط نفسه بالبرامج الأخرى وكذلك القدرة على إعادة تكرار نفسه بحيث يتوالد ويتكاثر، مما يتيح له فرصة الانتشار داخل جهاز الحاسب في أكثر من مكان في الذاكرة ليدمر البرامج والبيانات الموجودة في ذاكرة الجهاز.

وتكمن خطورة الفيروس في أنه مثله مثل الفيروس الذي يصيب الجسم الإنساني قادر على الانتقال من جهاز إلى آخر بسرعة كبيرة، ومن المفارقات أن ازدياد خطورته في الآونة الأخيرة جاء نتيجة التقدم الكبير الذي وصلت إليه وسائل الاتصال وشبكات الحاسب مما أدى إلى سهولة الاتصال بين أجهزة الحاسب وبعضها فمعظم الشركات والجهات الحكومية والجامعات

والمدارس الآن لديها شبكات محلية تربط بين العديد من أجهزة الحاسب، وكثير من هذه الجهات تتصل مع بعضها، بل كثيرًا ما تكون أجهزة الحاسب على اتصال برغم كونها في قارات متباعدة، وأوضح مثال على ذلك شبكة (إنترنت) التي تغطي العالم كله ولذلك يمكن للفيروسات أن تنتشر بسهولة وسرعة. ومن المفارقات كذلك أن توافق نظم التشغيل واتباعها للمعايير أدى بغير قصد إلى زيادة انتشار الفيروسات حيث يستطيع البرنامج الواحد الآن أن يعمل على أنواع مختلفة من الحاسبات ونسخ مختلفة من نظام التشغيل، والعامل الثالث الذي أدى إلى زيادة انتشار الفيروسات هو قرصنة البرامج التي جعلت نسخ البرامج غير الأصلية موضع التداول بين الكثير من الأجهزة، مما أوجد ثغرة كبيرة تنفذ من خلالها البرامج الملوثة بالفيروسات.

وليس ببعيد ما تسبب فيه الفيروس المعروف باسم (بطاقة عيد الميلاد Christmas Card) الذي ضرب الأجهزة في العالم كله وانتشر بسرعة مذهلة ، وهذا الفيروس يقوم بعرض بطاقة جميلة ملونة للتهنئة بأعياد الميلاد لدى المسيحيين، وفي نفس الوقت يقوم بقراءة العناوين المخزنة في الحاسب الذي دخل إليه ثم يقوم بإرسال نسخة من نفسه إلى هذه العناوين عن طريق البريد الإلكتروني. وهكذا بموالاة انتقاله من حاسب إلى آخر يتمكن في كل مرة من نسخ نفسه إلى عشرات الحاسبات الجديدة التي يتصادف وجود عناوينها في الحاسب الذي يصل إليه، وفي النصف الأخير من تسعينيات القرن العشرين انتشر هذا الفيروس وأشباهه عبر شبكة (الإنترنت) بشكل وبائي. وحدث أن استقبل طالب بكلية شهيرة بإحدى جامعات الخليج هذه البطاقة على الحاسب الخاص به، ولما تصادف في ذلك العام تزامن أعياد الميلاد مع شهر رمضان المعظم ، فقد قرر الطالب بحسن نية أن يحول هذا البرنامج إلى برنامج للتهنئة بشهر رمضان المبارك وقام بتغيير الرسوم والرموز الموجودة بالبطاقة إلى رسوم ورموز مناسبة لشهر رمضان ثم أعاد إرسال هذه الرسالة إلى أصدقائه دون أن يعلم أنه إنما يرسل فيروسًا شديد

الفتك. ومن سوء الحظ أن هذا الفيروس الجديد، والذي أطلق عليه اسم "فيروس رمضان"، قد تفوق على الفيروس الأصلي "بطاقة عيد الميلاد" في الانتشار مما أثار حنقًا شديدًا في العالم ، خاصة بعد اكتشاف الخبراء للجامعة التي انطلق منها بعد التتبع الدقيق لمصدر هذا الفيروس، وقد تلقينا في ذلك الوقت العديد من الرسائل الهجومية من خلال شبكة (إنترنت) توجه الاتهام بسوء التصرف.

نوع آخر من الفيروسات ليس بعيدًا عن هذا النوع وهو يتمثل في الرسالة التي وصلت إلى الملايين من المشتركين في شبكة (الإنترنت) في أول أبريل من عام ١٩٩٩م تدعي أن هناك طفلاً صغيرًا مريضًا بسرطان الدم وأنه يعالج في إحدى المستشفيات بالولايات المتحدة وأن المبلغ المرصود لعلاجه قد نفد وأن المستشفى سيضطر إلى إيقاف علاجه ما لم يصل إلى المستشفى عدد كاف من الرسائل التي تطالب باستمرار علاجه وأن المستشفى قرر إضافة مبلغ عشرة سنتات إلى الرصيد المخصص لعلاجه عن كل رسالة إلكترونية تصل إلى المستشفى، وتتضمن الرسالة الفيروسية نموذجًا للرسالة وتطلب من كل من تصله هذه الرسالة إعادة إرسالها إلى أكبر عدد من البشر حتى يمكن ضمان الوصول إلى مبلغ المليون دولار المطلوب لعلاج هذا الصبي المسكين! وتكون النتيجة بالطبع ملايين الرسائل التي تنهال عبر الشبكة.

هذه الأنواع من الفيروسات التي تحدثنا عنها لا تحدث ضررًا مباشرًا للبيانات المخزنة على الجهاز ولكنها بسبب تضاعفها الرهيب تتسبب في ضرر أكبر وهو زيادة كثافة المرور بالشبكة بشكل أدى في كثير من الأحوال إلى تأخر الاتصالات، بل إلى توقف بعض الشبكات عن العمل بالكامل وضياع بعض الرسائل المتبادلة والتي ربما قد تكون على جانب كبير من الأهمية.

٤-٢- نظرة من الداخل

هل هذا هو اليوم الموعود؟ إنني أعرف أنه من المفروض أن أفعل شيئًا هامًا اليوم إذا كان اليوم هو اليوم المنتظر. كلا .. إنه ليس الجمعة الموافق الثالث عشر من الشهر.. إذًا فاليوم لم يأت بعد.. حسنًا طالما أن اليوم ليس هو اليوم الموعود فيجب أن أعيد نسخ نفسي مرة أخرى. دعنا نلقي نظرة على ملفات النظام.. أعلم جيدًا أن هناك على الأقل واحدًا منها، فكل كمبيوتر لديه ملف نظام. حسنًا هذا هو.. هل هناك نسخة مني موجودة في هذا الملف؟ إذا لم تكن هناك نسخة مني فعليّ أن أقوم بإعداد نسخة من نفسي وإدخالها إلى هذا الملف. كلا.. إنني بالفعل متواجد في هذا الملف. إذا دعنا الآن نختبر ملفات البرامج في هذا الكمبيوتر. لابد وأن هناك برنامجًا واحدًا على الأقل لا يحمل بصمتي أو ليس لي تواجد فيه. نعم هذا هو.. لقد وجدته بعد (٤٨) محاولة فقط. ولكن يا للحظ العاثر إنه ملف (للقراءة فقط) أي أنني لن أستطيع الدخول إليه. ولكن لا توجد مشكلة، سوف أقوم بتغيير هذه الخاصية (خاصية القراءة فقط) بحيث أستطيع الدخول إلى البرنامج وتغييره. الآن أستطيع أن أضع نسخة مني في هذا البرنامج، ودعنا كذلك نغير قليلاً من أداء هذا البرنامج، فلنغير من خط سير البرنامج فنجعله يقفز قفزة صغيرة إلى هناك ثم يعود إلى المكان التالي لمكان دخولي. والآن ماذا نسيت؟ .. نعم لابد من إعادة خاصية القراءة فقط إلى ما كانت عليه قبل دخولي حتى لا يشعر أحد بما فعلت. والآن هل محوت آثاري تمامًا؟ دعنا نرى.. الخصائص كلها عادت كما كانت قبل دخولي إلى البرنامج، وحجم البرنامج لم يتغير فإنني أذكى من أن أترك هذا الأثر ورائي فقد وجدت مجموعة من المواضع الخالية في البرنامج، فقمت بحذف كمية منها مساوية لحجمي أنا. آه .. لقد كدت أنسى أن أعيد تاريخ تعديل البرنامج إلى ما كان عليه قبل دخولي. هذه السقطة كانت كفيلة بأن تكشفني. والآن هل انتهيت؟

كلا.. كلا. يجب الآن أن أكرر نفس الإجراء بالنسبة لباقي أجزاء القرص الصلب وكذلك بالنسبة للقرص المرن إذا كان هناك قرص في الجهاز. والآن إلى الجزء الممتع والمهم من جولتي.. فلنر إذا كنت أستطيع الوصول إلى الشبكة كذلك. سيكون ذلك عملاً عظيمًا بحق. هل انتهيت الآن؟ نعم. هذا ما يجب أن أفعله يوم الجمعة إذا وافق الثالث عشر من الشهر. كنت دائمًا تواقًا لمعرفة تأثير الأمر :Format C .. حسنًا من المفروض أن أصدر هذا الأمر بعد أن أقوم بإنشاء ٥٠ نسخة من نفسي، ولكنني الآن لم أنسخ سوى (٤٩) نسخة فقط.. إذًا لندع ذلك للمرة القادمة.

هذا هو "المنولوج" الذي تخيل "فيتز" حدوثه في كتابه "أزمة فيروسات الحاسب" [Fites 1992] على لسان فيروسه (ببعض التصرف من المؤلف). وربما كان هذا التخيل أفضل من أن نقدم خريطة مسار لتصرف الفيروس طالما أن الفيروسات لا تلتزم خريطة مسار واحدة.

١-٣- كيف كانت البداية؟

من الصعب أن نحدد بشكل دقيق وموثق كيف بدأت الفيروسات بالظهور، وهي في ذلك شأنها شأن الموروثات الشعبية أو قصص ألف ليلة وليلة أو الحكم والأمثال التي يصعب معرفة مؤلفها أو من كان أول من حدث بها. وتزداد الصعوبة في الأمور التي لا يفخر الإنسان بارتكابها، مثل صنع الفيروسات. ولكن الرواية الأقرب إلى التصديق هي أن القصة بدأت في باكستان، ويدعم هذه الرواية أن الفيروس الباكستاني كان من أوائل الفيروسات التي تم اكتشافها في أواخر السبعينيات من القرن العشرين. والرواية تقول إن أحد أصحاب محال بيع البرامج في باكستان، والذي لم يكن يتقيد بحقوق النشر، كان يشتري نسخة أصلية من أي برنامج ثم ينسخ منها نسخًا عديدة كان يبيعها لزبائنه بسعر منخفض، ويكسب بذلك الكثير. ثم

اكتشف هذا الرجل أن بعض منافسيه كانوا يشترون منه النسخة المقلدة منخفضة السعر ثم ينسخونها بدورهم ويبيعونها بأسعار منافسة مما أدى إلى تدهور تجارته. ولذلك فكر في إضافة كود بسيط إلى الأقراص التي يبيعها لمنافسيه مما يجعلها لا تعمل عند محاولة تشغيلها وبذلك يفقد العملاء ثقتهم في منافسيه ولا يقبلون إلا على بضاعته!

وهناك من يؤكد أن أول فيروس ظهر في أواخر الخمسينيات أو أوائل الستينيات من القرن العشرين كتجربة أثناء عملية تصميم نظم التشغيل [Cohen 1992] ، وفي السبعينيات ظهرت "دودة زيروكس" وأظهرت قدرتها على التغلغل في بعض الشبكات، وقد سببت هذه الدودة انقطاع خدمات هذه الشبكات. ولكن لم تتخذ إجراءات جدية نحو مقاومة الفيروسات حتى عام ١٩٨٤م عندما نشر "فردريك كوهين" ورقة العمل الشهيرة في أحد المؤتمرات العلمية لتفتح هذا المجال.

أيًا كانت البداية، فقد انتشرت الفيروسات بالفعل وساعد على انتشارها أن طريقة كتابة برامج الفيروسات سهلة، بل إنها منشورة في بعض الكتب. وهناك مواقع على شبكة (الإنترنت) تشرح بالتفصيل كيفية كتابة الفيروس وكيف يمكن أن تجعله أكثر ضراوة وأشد إيذاء !

٢- أنواع الفيروسات

تأخذ الفيروسات أشكالاً عديدة فقد تشبه الدودة في توالدها وتكاثرها، وقد يتم إدخالها إلى النظام لتحدث التخريب المطلوب في توقيت معين أو عند حدوث واقعة معينة. وفيما يلي بعض أشكال الفيروسات:

٢-١- حصان طروادة (Trojan Horse)

هو جزء صغير من الكود يضاف إلى البرمجيات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرمجيات ولكنه يؤدي عملاً تخريبيًا

للنظام، وتكمن خطورته في أن النظام لا يشعر بوجوده حتى تحين اللحظة المحددة له ليؤدي دوره التخريبي.

٢-٢- القنابل المنطقية (Logic Bombs)

القنبلة المنطقية هي أحد أنواع حصان طروادة وتصمم بحيث تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين، فقد تصمم بحيث تعمل عند بلوغ الموظفين في الشركة عدداً معيناً من الموظفين مثلاً، أو إذا تم رفع اسم المخرب (واضع القنبلة) من كشوف الرواتب، وتؤدي القنبلة في هذه الحالة إلى تخريب بعض النظم أو إلى مسح بعض البيانات أو تعطيل النظام عن العمل.

٢-٣- القنابل الموقوتة (Time Bombs)

القنبلة الموقوتة هي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة أو في يوم معين كأن تحدث مثلاً عندما يوافق اليوم الثالث عشر من الشهر يوم جمعة.

٢-٤- باب المصيدة (Trapdoor)

هذا الكود يوضع عمدًا بحيث يتم -لدى حدوث ظرف معين- تجاوز نظم الحماية والأمن في النظام. ويتم زرع هذا الكود عند تركيب النظام بحيث يعطي المخرب حرية تحديد الوقت الذي يشاء لتخريب النظام فهو يظل كامنًا غير مؤذٍ حتى يقرر المخرب استخدامه، وكمثال على ذلك إقحام كود في نظام الحماية والأمن يتعرف على شخصية المخرب ويفتح له الأبواب دون إجراء الفحوص المعتادة.

٢-٥- الديدان (Worms)

الدودة هي عبارة عن كود يسبب أذىً للنظام عند استدعائه، وتتميز

الدودة بقدرتها على إعادة توليد نفسها، بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث. وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة، وهكذا تنتشر الدودة وتتوالد.

٢-٦- فيروس التلصص على البريد الإلكتروني

أعلنت جامعة "كارنيجي ميلون" في تصريح وزعته وكالة "أسوشيتد برس" في ١٩٩٩/٣/٢٨م عن فيروس يهاجم الرسائل المرسلة عبر البريد الإلكتروني فيقوم بنقل نسخة من هذه الرسائل إلى أشخاص آخرين دون إذن من أصحابها. وقال المتحدث باسم الجامعة أن هذا الفيروس المسمى "ميليسا ماكرو" أو "ميليسا دبليو ٩٧ إم" ينتشر من خلال البريد الإلكتروني فيهاجم أجهزة الحاسب المحملة ببرامج "مايكروسوفت" التي تستخدم على نطاق واسع مثل "وورد ٩٧" أو "وورد ٢٠٠٠" فيقوم بنقل بعض الوثائق المخزنة باستخدام هذه البرامج إلى الجهة المتلصصة. وقد نشرت جريدة الرياض السعودية في عددها الصادر في ٢٨ أغسطس ١٩٩٩م أن مبرمج فيروس "ميليسا" واسمه "ديفيد سميث" ويبلغ من العمر ٣٠ عامًا قد اعترف أمام إحدى المحاكم الأمريكية في ولاية "نيوجيرسي" بأنه قام ببرمجة هذا الفيروس في شهر مارس ١٩٩٩م. وأضافت الصحيفة أنه من المتوقع صدور قرار المحكمة خلال شهر، وأنه يواجه عقوبة قد تصل إلى (٤٠) سنة سجن وغرامة تصل إلى نصف مليون دولار إذا ما ثبتت جميع التهم الموجهة ضده.

ونحن لا نستطيع أن نؤكد أو ننفي تورط أجهزة الاستخبارات الدولية في مثل هذه الأعمال لأن الاستفادة من مثل هذه الوثائق وعلى هذا النطاق العالمي لا يمكن أن تتم إلا من خلال مثل هذه المؤسسات التي لديها القدرة على جمع هذا الكم الهائل من المعلومات وتحليلها.

٢-٧- فيروسات تصيب العتاد

لا يقتصر نشاط الفيروسات على إصابة البرامج أو تدميرها فقط ولكن تم تطوير أنواع من الفيروسات يمكن أن تصيب العتاد، وأحد هذه الفيروسات هو برنامج يقوم بتنفيذ ملايين العمليات الحسابية المتوالية بدون استخدام أوامر للإخراج أو الإدخال مما يلقي عبئًا كبيرًا على وحدة المعالجة المركزية (CPU) فترتفع درجة حرارتها بشكل مطرد ولا تتاح لها فرصة من خلال أوامر الإدخال والإخراج كي تبرد. وبذلك بعد بضعة دقائق تحترق وحدة المعالجة المركزية. ونود التنبيه هنا إلى أنه لم تثبت حتى الآن حالات من هذا القبيل.

٣- طرق الوقاية من الفيروسات

٣-١- تصنيف طرق الوقاية

إذا أردنا وضع تصنيف لطرق الوقاية من الفيروسات فيمكننا وضع التصنيفات التالية لأساليب أو طرق الوقاية:

١) تعقب آثار الفيروس

يمكن باستخدام أسلوب التوقيع الرقمي تتبع آثار الفيروس إلى مصدره وذلك من خلال استخدام (Audit Trail). ومن شأن ذلك أن يحجم مروجو الفيروسات عن إنتاجها وترويجها، وأن يتوخى الجميع الحذر في هذا الصدد .[Cohen 1992]

٢) أمصال التطعيم

يترك الكثير من الفيروسات في البرامج المصابة معلومات عنها أو آثار لها وذلك لمنع إعادة إصابة هذه الفيروسات مرة أخرى لأنه لا ضرورة

لذلك، وقد استطاع متخصصو أمن المعلومات المهتمون بمقاومة الفيروسات صنع "أمصال" خاصة للتطعيم (Vaccines). وتقوم هذه الأمصال بتقليد عملية الإصابة بالفيروس وذلك بأن تضع هذه المعلومات التي يتركها الفيروس لعدم الإصابة في نفس المواضع التي يضع الفيروس فيها هذه المعلومات. ولكن هذا الأسلوب من الدفاع يمكن هزيمته بسهولة إذا تعرض البرنامج لفيروس مختلف.

٣) الدفاع الذاتي للبرامج

يستطيع كل مبرمج تصميم نظام دفاعي ضد الفيروسات، وهناك أبحاث تقترح أن تضاف هذه الإمكانية لمترجمات البرامج (Compilers) وذلك حتى تقوم بتزويد البرامج في مرحلة الترجمة بهذا النظام الدفاعي. وتكمن ميزة هذا الأسلوب في سهولة وسرعة تطبيقه، ولكن يعيب هذا الأسلوب أنه لا يستطيع اتخاذ إجراء ضد الفيروس المهاجم إلا بعد تعرفه على هذا الفيروس، وربما يكون الوقت عندئذ قد فات وبدأ الفيروس نشاطه الهدام.

٤) حصر الصلاحيات

آليات الحماية في معظم النظم لا تتم صيانتها بشكل جيد من جانب مسئولي أمن النظام. فتجد بعض مسئولي أمن النظام يمنحون صلاحيات عديدة لكثير من المستفيدين إما بشكل منفرد أو كمجموعات، وتتسع هذه العملية يومًا بعد يوم وتتعدد الصلاحيات الممنوحة حتى يصبح من الصعب حصر كل من له صلاحية التعديل على البرامج أو الملفات أو قواعد البيانات. من السهل في هذه الظروف أن تنتشر الفيروسات وبحصر الصلاحيات ومتابعتها يمكن أن ننشئ حائطًا دفاعيًا مبدئيًا في مواجهة الفيروسات. كما يجب قصر حق تعديل الملفات على أقل عدد ممكن من المستفيدين.

٥) توعية المستفيد

يعتبر وعي المستفيد حجر الزاوية في جهود الحماية ضد الفيروسات فوعيه بالأخطار التي تهدده سوف يجعله أكثر حذرا وأكثر حرصًا وأكثر اتباعًا للتعليمات [Jackson 1992]. ويمكن أن نستخدم نظام التشغيل في التوعية فيمكن مثلاً عند حدوث أي تعديل على ملف ما أن يقوم نظام التشغيل بإخطار المستفيد صاحب الملف بهذا التعديل. وهذا الإخطار في حد ذاته يجعل المستفيد أكثر انتباهًا للمسألة فتدخل إلى دائرة وعيه.

٦) تعدد الوسائل

صحيح أنه لا توجد وسيلة حاسمة تستطيع الكشف عن جميع الفيروسات، ولكن استخدام وسائل متعددة يشبه تمامًا وضع عوائق متعددة أمام المهاجم.

٣-٢- إجراءات من جانب الفرد

يستطيع مستخدم الحاسب الشخصي اتخاذ بعض الإجراءات التي تحمي إلى حد كبير بياناته الهامة ومنها:

١) احتفظ بنسخ احتياطية من البرامج والبيانات مأخوذة على فترات متقاربة.

٢) احتفظ بهذه النسخ وبأصول البرامج في مكان آمن بعيدًا عن الحاسب الشخصي.

٣) احتفظ بسرية كلمة المرور وقم بتغييرها من وقت لآخر.

٤) أغلق الجهاز قبل أن تترك مكانك أمامه.

٥) قم بتركيب نسخة حديثة من أحد برامج مكافحة الفيروسات.

٦) احتفظ لديك بالرقم المتسلسل للجهاز وللقرص الصلب.

٧) لا تقم بتحميل أي بيانات شخصية دون التنسيق مع مسئول أمن المعلومات.

٨) عند حدوث مشكلة أو الشك بوجود فيروس اتصل فوراً بمسئول مساندة المستفيدين، وأخطره بما حدث وبما قمت به من إجراءات.

٩) ضع شريط الحماية أو أغلق فتحة التأمين للأقراص المرنة بعد الانتهاء من استخدامها لمنع الكتابة عليها بشكل غير مقصود.

١٠) افحص البرامج الجديدة قبل استخدامها للتأكد من خلوها من الفيروسات.

١١) تأكد عند شراء البرمجيات الجديدة من أن الصندوق لم يفتح من قبل.

١٢) لا تستخدم النسخ المقلدة أو المنسوخة من البرامج.

١٣) عند إعادة استخدام أقراص مرنة قديمة، قم بتهيئتها (Format) بدلاً من مجرد مسحها (Delete).

٣-٣- إجراءات من جانب المنشأة

هناك عدة إجراءات وقائية عند تطبيقها تعفي المنشأة من كثير من العواقب الوخيمة التي قد تترتب على الإصابة بالفيروسات مثل:

١) إعداد نسخة المصدر (قبل الترجمة) من البرامج المطورة داخليّا أو النسخة الأصلية من البرمجيات المشتراة وحفظها في مكان آمن بحيث يمكن استرجاع نسخة نظيفة (غير ملوثة بالفيروس) من البرنامج عند

الحاجة.

٢) الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات بحيث يتم تسجيل جميع وقائع نقل البرامج المعدلة إلى البيئة الإنتاجية، وبخاصة تلك البرامج المجلوبة من خارج المؤسسة.

٣) توعية المستخدمين بعدم تحميل أي برنامج مجلوب من الخارج في حاسباتهم الشخصية، فهذا هو أوسع الأبواب لإدخال الفيروسات إلى النظم والتي عند دخولها ربما تصيب جميع الأقراص وجميع الأجهزة بالشبكة. والبرامج المجانية التي تنتقل من يد إلى يد أو يتم توزيعها بواسطة مجلات الكمبيوتر المتخصصة يجب دائمًا الحذر في التعامل معها، حتى تلك البرامج التي تأتي من مصادر لا يرقى إليها الشك يجب فحصها جيدًا.

٤) عدم إجازة البرامج للاستخدام العام في المؤسسة، وخاصة تلك التي يتم تركيبها على الشبكة المحلية، إلا بعد اجتيازها بنجاح الاختبارات اللازمة للتأكد من خلوها من الفيروسات، وبعد ذلك يتم تأمينها ضد الكتابة أو التعديل.

٥) عند فحص البرمجيات أو اختبارها قبل السماح بنشرها في المؤسسة للاستخدام العام، يجب أن يتم ذلك على جهاز مستقل غير مرتبط بالشبكة. ويفضل أن يكون هذا الحاسب مجهزا بحيث يعمل بتاريخ ثابت يتفادى بعض التواريخ التي تنشط فيها الفيروسات بناء على التعليمات المخزنة فيها قبل الجمعة ١٣ نوفمبر أو ١٥ أبريل أو غير ذلك من التواريخ التي

دأب صانعو الفيروسات على إدراجها في برامجهم، ويجب أن يتضمن الاختبار البحث عن أي سلوك غير مفهوم في البرنامج كأن يخرج رسائل لا داعي لها على الشاشة مثلاً، ولو أن خلو البرنامج من مثل هذا السلوك غير المفهوم لا يعني بالضرورة نظافة البرنامج فالفيروسات تظل كامنة ولا تكشف عن سلوكها إلا في اللحظة المناسبة.

٦) تركيب برنامج على الشبكة الداخلية وأجهزة الحاسب الرئيسية للتحقق من وجود فيروسات ويفضل أن يكون هذا البرنامج دائم الوجود في الذاكرة، وهذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة لها، ولذلك فهي تكون عديمة الفائدة في مواجهة الفيروسات الجديدة. ولذلك يجب تحديث هذه البرامج باستمرار ، ويفضل استخدام البرامج التي تقوم آليًا بمقارنة محتويات بعض مناطق القرص (الصلب أو اللين) أو بعض مناطق الذاكرة بمحتوياتها المتوقعة والمفترض أن توجد فيها والإبلاغ عن أي تغير فيها مما قد ينبئ عن وجود فيروس، وبعض هذه البرامج يقوم بذلك آليًا عند بدء تشغيل البرامج أو بدء استخدام الأقراص المرنة.

٧) اتخاذ الإجراءات اللازمة لتقييد تشغيل الحاسبات الشخصية من القرص المرن قد تصل إلى إلغاء وحدة إدارة الأقراص المرنة كلما أمكن ذلك والاكتفاء بالقرص الصلب عند ربط هذه الحاسبات بالشبكة المحلية.

٨) اتخاذ إجراءات في مواجهة المتصلين من خارج المؤسسة للتأكد من

خلو البرامج المدخلة من جانبهم من الفيروسات.

٩) وضع برنامج عازل للفيروسات في الجهاز الذي يصل بين الشبكة الداخلية والعالم الخارجي (مثل الوسيط Proxy) لمنع وصول الفيروسات إلى الشبكة المحلية أو إلى أجهزة المستفيدين.

١٠) التأكد من أن جميع الاتصالات التي تتم من خلال الحاسبات الشخصية للمستفيدين بخارج المؤسسة تتم عن طريق الشبكة وليس عن طريق مودم قد يتم تركيبه خلسة في أحد الحاسبات الشخصية للاتصال (بإنترنت) مثلاً.

١١) تدريب الموظفين على كيفية الوقاية ضد الفيروسات والتعامل معها عند العثور عليها ومعالجة آثارها.

١٢) أخذ نسخ احتياطية من البيانات على فترات منتظمة ومعلومة ومعلنة للجميع ومن ثم حفظها في مكان آمن.

١٣) تحديد مسئولية التعامل مع البيانات وتسجيل وقائع استخدام الملفات وقواعد البيانات.

١٤) نشر إجراءات محددة وواضحة على المستفيدين لاتباعها في حالة ظهور فيروس لديهم.

١٥) عدم السماح بنسخ البرمجيات الأصلية بواسطة الموظفين سواء بحجبها عنهم أو بإصدار التعليمات بذلك.

١٦) عدم السماح بنقل الملفات أو البرامج على أقراص مرنة بواسطة

الموظفين الذين قد يريدون مواصلة العمل في المنزل، وذلك لعدم ضمان خلو حاسباتهم الشخصية بالمنزل من الفيروسات.

١٧) عدم السماح للموظفين بحماية الملفات الحساسة بواسطة كلمة سر خاصة بهم حتى يمكن الدخول إلى هذه الملفات وفحصها عند الحاجة.

١٨) يؤكد "هايلاند" في كتابه الشهير "مرجع فيروسات الحاسب" [Highland 1990] أن دور مدير مركز الحاسب الآلي في مكافحة الفيروسات يختلف عن دور الإدارة العليا، فبينما يطلب من الإدارة العليا الدعم المالي والمعنوي فإن مهمة التخطيط والمتابعة والتفتيش تقع على عاتق مديري الحاسب.

٣-٤- إجراءات ذات طابع أشمل

٣-٤-١- التوقيع الرقمي

لما كان تداول البيانات داخل الشبكات والبريد الإلكتروني هما من المصادر الهامة للإصابة بالفيروسات فلابد من التركيز على هذا القطاع للحد من تأثير الفيروسات وذلك بالعمل على اكتشاف وجودها قبل أن تبدأ عملها. وأحد الأساليب الفعالة لتحقيق ذلك هو أسلوب استخدام (التوقيع الرقمي Digital Signature) والتي سوف نتعرض لها بالتفصيل عند الحديث عن البريد الإلكتروني. وأسلوب عمل التوقيع الرقمي يختلف عن أسلوب البرمجيات التي تستخدم للكشف عن وجود الفيروس، ولكنه يسمح بكشف أي تغيير قد يتم إجراؤه على أي برنامج أو ملف، ذلك لأنه ببساطة يشبه توقيع مرسل الرسالة عليها ولا يمكن تزويره أو افتعاله. وقامت بعض الشركات الصانعة للبرمجيات بتقديم العديد من المقترحات [Bidzos 1992] بهدف

تعميم استخدام التوقيع الرقمي في جميع معاملات البريد الإلكتروني على شبكة (إنترنت) وكذلك في شبكات (إنترانت) وهي الشبكات المحلية الداخلية في المنشآت والتي تستخدم تقنية (إنترنت) من برمجيات مثل (HTML) وصفحات (Web) و(متصفح Browser) وغير ذلك. ومن بين هذه المقترحات أن تقوم الشركات الصانعة للبرمجيات (بالتوقيع) رقميًا على منتجاتها، مما يسمح لمستخدم البرنامج بالتعرف على أي تعديل قد يكون ألحق بالبرنامج بعد إنتاجه. وفي حالة تلوث البرنامج بأحد الفيروسات يمكن، من خلال التوقيع الرقمي، تتبع هذا الفيروس حتى مصدره مما يشكل حافزًا قويًا لمطوري البرامج لتوخي الحذر عند تطوير وإنتاج برامجهم. ومن خلال التوقيع الرقمي يمكن أن يتحقق نظام التشغيل من صحة التوقيعات على البرامج قبل السماح بتشغيلها، وبذلك تتضاءل فرص النجاح أمام أي فيروس، ولو أن هذا قد يؤدي إلى سوء الأداء في الحاسبات البطيئة ، ولكن بعد ازدياد سرعات الحاسبات الشخصية والوصول إلى سرعة (١) جيجا بايت، فإن ذلك يجعل هذه العملية ذات تأثير لا يكاد يذكر على الأداء.

٣-٤-٢- توحيد المعايير

يدعو "لو" في كتابه "التعامل مع فيروسات الحاسب" [Louw 1992] إلى إيجاد معايير موحدة للتوثيق وأسلوب توزيع البرمجيات التي تنتجها الشركات لضمان الحد من انتشار الفيروسات.

٣-٤-٣- دور القوانين والتشريعات

ما هي الحماية التي يكفلها القانون أو التشريعات القانونية في مواجهة انتشار الفيروسات، لاشك أن العالم الغربي يوفر بعض الضمانات، مثل: التعويضات المادية عن الخسائر المثبتة أو معاقبة المجرمين في حالة التوصل إليهم. ولكن التشريعات دائمًا ما تأتي متأخرة بعض الوقت حتى يتم استيعاب كافة الاحتمالات ودراسة السوابق وغير ذلك من المراحل التي تمر بها

التشريعات حتى تصدر. ولكن هل هناك في العالم العربي مواد واضحة في قانون العقوبات تجرم عمليًا نشر الفيروسات ونحن نعلم أنه لا عقوبة بغير نص؟ في الواقع لم يصل بحثنا إلى أي عقوبات واضحة تتحدث عن عملية نشر الفيروسات، وإنما ما هو قائم هي عملية تطويع أو تكييف لا غير للقوانين الحالية التي تتصدى للغش أو التزوير أو تخريب ممتلكات الغير. ولذلك فإننا نظن أنه من الضروري أن تكون هناك نصوص واضحة ومنشورة تتضمن العقوبات التي توقع في حالة ضبط شخص وإدانته بجريمة نشر الفيروسات، ويجب أن يؤخذ في الاعتبار أن الجرائم من هذا النوع هي جرائم يصعب إيجاد الدليل عليها أو تقديم الشهود على حدوثها.

٣-٥- عيوب الرقابة الأمنية الصارمة

تتجه معظم الإجراءات المضادة بصفة عامة للحد من عدد مستخدمي المعلومات، والسبب طبعًا هو أن السلوك المعيب لنفر من الناس يمكن أن يفسد الأمر على الأغلبية التي تلتزم بالسلوك القويم. ولكن النظم التي تعودت في السابق على الدخول المفتوح أو غير المقيد إلى البيانات ستتأثر سلبًا بهذه الإجراءات. ويعتقد بعض الباحثين أن فرض الإجراءات الرقابية الصارمة تشكل بصفة عامة قيدًا على ملكة الابتكار لدى العاملين [Abrams 1998].

من الضروري أن يدخل أمن الحاسبات، وهو الذي يتكون في غالبه من إجراءات سرية البيانات وسلامتها، في نسيج دورة حياة تطوير نظم المعلومات أي يجب أن يدخل في جميع مراحل هذه الدورة، وعادة ما يشكل ذلك عبئًا على العمل من جميع النواحي سواء الفنية أو الإدارية أو التنظيمية أو يكون حتى عبئًا على مستوى الأداء. وقد يكون من الصعب في بعض الأحيان إضافة أنواع معينة من إجراءات الأمن للنظم القائمة بالفعل بعد أن انتهى تطويرها.

كثيرًا ما تكون الإجراءات الأمنية غير مقبولة من جـــانب المســتفيد، بالإضافة إلى ما قد تضيفه من تكلفة مادية، ومن المعتاد أن ينتـــهي الأمـــر بتحمل المستهلك تكلفة تأمين نظم المعلومات للشركات التي تنتج السلعة التـــي يشتريها ولكن يؤكد "أبرامز" أن المستقبل، الذي من المؤكد أن يشهد انتشـــارا كبيرًا للتجارة الإلكترونية، سيخفض من تكلفة السلعة على المستهلك مما يتيح الفرصة لتعويض الإنفاق المتزايد على أمن المعلومات. ذلك الإنفـــاق الـــذي ينشأ عن تأمين عمليات التجارة الإلكترونية وحمايتها من العديد من الأخطار التي تتعرض لها ومن بينها الفيروسات [Abrams 1998] .

٤- طرق علاج آثار الفيروسات

١) عند اكتشاف برامج ملوثة ضمن برامج التطبيقات يجب إزالتها فورًا، فإذا تم الاكتشاف في الوقت المناسب فيمكن أن نحل محلها النسخة النظيفة من البرنامج المحفوظة لدى المؤسسة، أما إذا تم اكتشافها بعد فـــوات الأوان فمن الضروري في هذه الحالة فحص مكتبة البرامج كلها بعناية وإزالـــة أي برامج دخيلة.

٢) إذا كان التخريب عن طريق حذف بعض برامج التطبيقات فعادة يكـــون الاحتفاظ بالنسخة الورقية للبرامج (قائمة المصدر للبرنامج) مفيدًا حتى لو كانت هذه النسخة الورقية تمثل إصدارًا قديمًا من البرنامج فيمكـــن عـــن طريقها استعادة البرنامج المحذوف.

٣) بعد حدوث أي حالة تخريب يجب فحص قائمة البرامج الموجـــودة فـــي الأجهزة المختلفة ومقارنتها بالقائمة السابقة على عملية التخريب لاكتشاف أي برامج دخيلة وذلك بالتأكد من أسماء البرامج وأحجامها وتاريخ آخر تعديل عليها، أما إذا كان التخريب الذي وقع في شـــكل تضميـــن كـــود مدسوس في بعض البرامج المشروعة، فإن وسيلة اكتشاف ذلـــك هـــي استخدام برامج اختبار خاصة أو بمقارنة الكود الموجود بعد التخريب مع نسخة سابقة نظيفة.

٤) إذا كانت البيانات هي التي تم تخريبها، فيجب في هذه الحالـــة فحـــص البيانات وإزالة أي تغييرات تكون قد طرأت عليها. فإذا كان التخريب قد تم اكتشافه في الوقت المناسب فيمكن إحلال نسخة قديمـــة نظيفـــة مـــن البيانات محل النسخة الملوثة، ومن ثم إعادة التشغيل من النسخة القديمـــة ثم العمل على تحديثها. أما إذا كان اكتشاف التخريب قد تم بعد مـــرور فترة طويلة وكان من الصعب العودة إلى نسخة سابقة من البيانات ففـــي هذه الحالة يجب طلب معونة أحد خبراء أمن البيانات لينضم لفريق العمل المكلف بمعالجة الموقف.

الفصل الخامس

مواجهة الكوارث

موضوعات الفصل:

(١) مبدأ استمرارية العمل.

(٢) أهمية التخطيط لمواجهة الكوارث.

(٣) الأخطار المحتملة المسببة للكوارث.

(٤) المبادئ الأساسية لنشاط مواجهة الكوارث.



في هذا الفصل نبدأ الحديث عن نشاط "مواجهة الكوارث" حيث نستهله بالحديث عن مبدأ استمرارية العمل ، حيث أن المهم هو أن يستمر العمل وألا يتأثر بالكارثة إلا في أضيق الحدود. نشير بعد ذلك إلى أهمية التخطيط المسبق لمواجهة الكوارث وماذا لو لم نلجأ إلى التخطيط، ثم نلخص الأخطار المحتملة التي تسبب الكوارث. ثم نختتم الفصل بتحديد المبادئ الأساسية لنشاط مواجهة الكوارث.

١- مبدأ استمرارية العمل

١-١- مفهوم الكارثة

المقصود بالكارثة (Disaster) من وجهة نظر نظم تقنيات المعلومات أنها أي حادث ينتج عنه تعطل نظام الحاسب عن العمل لمدة محسوسة.

والكوارث قد تنشأ عن أسباب طبيعية لا حيلة لنا فيها كالزلازل والأعاصير والفيضانات، أو بشكل متعمد مثل الحوادث الإرهابية، أو لأسباب أخرى فنية مثل أعطال الأجهزة أو أخطاء البرامج. ونذكر من هذه الكوارث:

١) زلزال سان فرانسيسكو.

٢) انقطاع الكهرباء الشامل في الرياض.

٣) فيضانات بنجلاديش.

٤) إعصار أندرو.

٥) تفجيرات الجيش الأحمر الأيرلندي في لندن.

وتظهر الإحصاءات أن السبب الرئيسي وراء الكوارث في مجال تقنية المعلومات والذي تستدعى من أجله الشركات المتخصصة في مواجهة

الكوارث هو انهيار النظام (System failure) ، فتبين الإحصاءات أن انهيار النظام هو المسئول عن ثلاثة من كل أربعة حوادث [Caelli 1989].

١-٢- معالجة الكوارث

المقصود بمعالجة الكوارث (Disaster Recovery) أنها قدرة المؤسسة عند حدوث الكارثة علـى تشـغيل الأنظمـة الضرورية لإنقـاذ العمـل واستمراريته.

وإذا لم تعالج الكارثة بشكل جيد فقد يكون ذلك سببًا في وقوع كارثـة أخرى في وقت لاحق، فحتى بعد نجاح عملية استعادة النشاط والعودة إلـى الحالة الطبيعية ستواجه المؤسسة :

١) قائمة طويلة من الأعمال المتأخرة المطلوب إنجازها.

٢) الكثير من تضارب البيانات في الملفات المختلفة.

٣) الكثير من الاستفسارات والكثير من المشكلات.

وربما انقضت سنة كاملة من الاضطراب المستمر، خلالها تكون هناك فرصة كبيرة لحدوث كارثة أخرى.

١-٣- استمرارية العمل

المقصود باستمرارية العمـل (Business continuity) أنـها قـدرة المؤسسة على الاستمرار في أداء أعمالها بمستوى مقبول من الكفـاءة بعـد وقوع حادث مفاجئ أو كارثة. وفي السنوات الأخيرة أصبح التركـيز علـى استمرارية العمل وليس على مواجهة الكوارث كما كان الاتجاه سـابقا، فقـد كان التخطيط في الماضي لمواجهة الكوارث مركزًا على قدرات الحاسب في المؤسسة، ومركزًا كذلك على العاملين في إدارة الحاسب الآلي دون غـيرهم،

أما الآن فقد تأكد أن المهم هو العمل الأساسي للمؤسسة، وأنه هو الذي يجب أن يستمر، وأن الحاسب ما هو إلا أحد الموارد المطلوبة للمحافظة على استمرار العمل، وبذلك امتد التركيز إلى المستفيد في المؤسسة بدلاً من الاقتصار على العاملين في إدارة الحاسب، والتركيز على احتياجات هذا المستفيد حتى يتمكن من المحافظة على استمرارية العمل. وقد غير هذا التحول في التفكير من أسلوب تصميم التطبيقات وإعدادها.

ولذلك تقوم كل مؤسسة بإعداد خططها الخاصة بالمحافظة على استمرارية العمل وفقًا للمتطلبات الخاصة للعمل الذي تقوم به، وتفضل بعض المؤسسات أن تنظر إلى التخطيط لاستمرارية العمل نظرة أكثر شمولاً بحيث تأخذ في الاعتبار كل الوظائف التي لديها وكل الإمكانات والموارد، فلا يكون الحاسب الآلي إلا واحدًا من هذه الموارد لا غير.

١-٤- احتمال حدوث الكارثة

لعل السؤال الصعب الذي يواجه جميع المؤسسات التي تمارس عملية التخطيط لاستمرارية العمل هو سؤال **الاحتمالية** : ما هو احتمال حدوث الكارثة؟ ومن الصعب الحصول على إحصاءات دقيقة في هذا المجال ، ولكن مؤسسات التأمين الفرنسية قامت بتحليل بعض الإحصاءات، ومن ثم ضمنتها في إحدى حزم البرمجيات الخاصة بتحليل المخاطر (Risk analysis) وهي برمجية (ماريون Marion) . كما اقترح "مارتن سميث" في كتابه (Common Sense Computer Security) أن احتمال وقوع الكارثة هو بالتقريب (١:٧٥٠) في السنة.[Martin 1989]، وعندما يطبق ذلك على دولة مثل المملكة المتحدة تضم حوالي ١٥,٠٠٠ مؤسسة كبيرة نجد أن هناك احتمالاً لوقوع (٢٠) حادثًا كبيرًا في العام، ونعني بالحادث الكبير أنه الحادث الذي يسبب اضطرابًا شديدًا في أعمال المؤسسة.

٢- أهمية التخطيط لمواجهة الكوارث

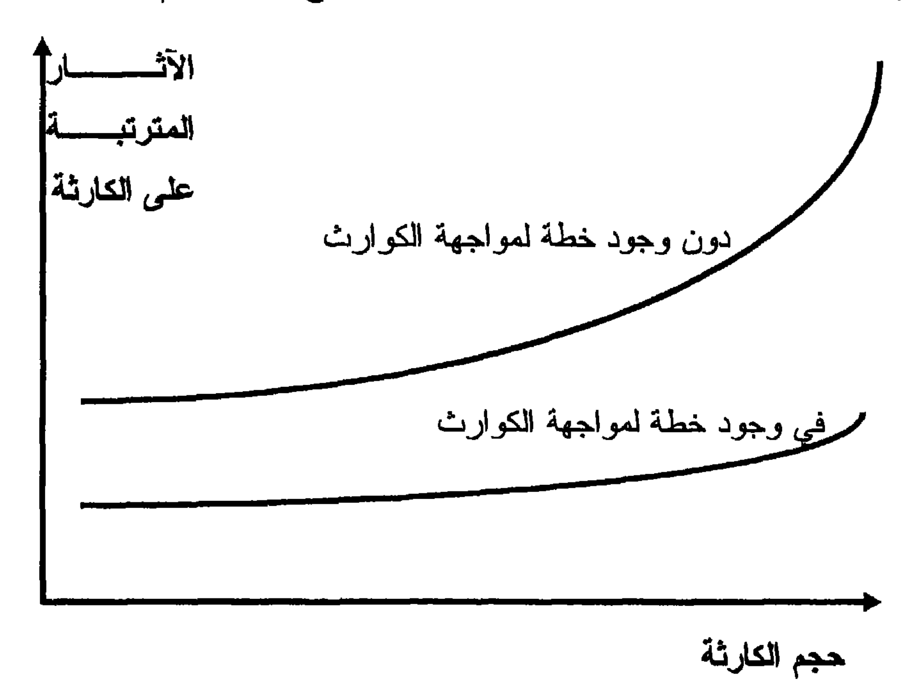
٢-١- لماذا نحتاج للتخطيط لمواجهة الكوارث؟

إننا نحتاج إلى التخطيط المسبق والجيد لمواجهة الكوارث -أو استعادة النشاط- (Disaster Recovery Planning) للأسباب التالية:

١) الاعتماد المتزايد في ميكنة العمل على تقنيات المعلومات.
٢) عدم كفاية البديل الاحتياطي اليدوي لاستعادة النشاط.
٣) لتقليل الخسارة المادية إلى حد محتمل.
٤) للمحافظة على ثقة المؤسسات الأخرى التي تتعامل مع المؤسسة.
٥) للمحافظة على الصورة الجيدة للمؤسسة.
٦) للإسراع في استعادة النشاط إلى ما كان عليه.
٧) لمواجهة الالتزامات القانونية.
٨) لمنع المنافسين من الاستفادة من الكارثة ، بل على العكس ربما يعطي وجود الخطة ميزة للمؤسسة إذا حدثت الكارثة.
٩) لإعادة العمليات الحرجة لأعمال المؤسسة أقرب ما يمكن لما كانت عليه في وقت متفق عليه وبتكلفة اقتصادية.
١٠) للتأكد من أن الكم المتراكم من البيانات الذي تجمع خلال توقف الحاسب وكذلك البيانات التي فقدت نتيجة الكارثة من الممكن جمعها من أجل إدخالها لاحقًا للأجهزة الاحتياطية.
١١) لتقليل الخسائر المباشرة أو غير المباشرة الناتجة عن تأخر أو توقف معالجة البيانات.
١٢) للتعامل بشكل مرضٍ مع الظروف التي تنشأ عن توقف العمل وتغيير الحاسبات والمواقع.
١٣) للاحتفاظ بعلاقات جيدة مع الموظفين.

١٤) لتقليل الفوضى التي قد تنجم عن الكارثة والسماح باستعادة النشاط بشكل سريع.

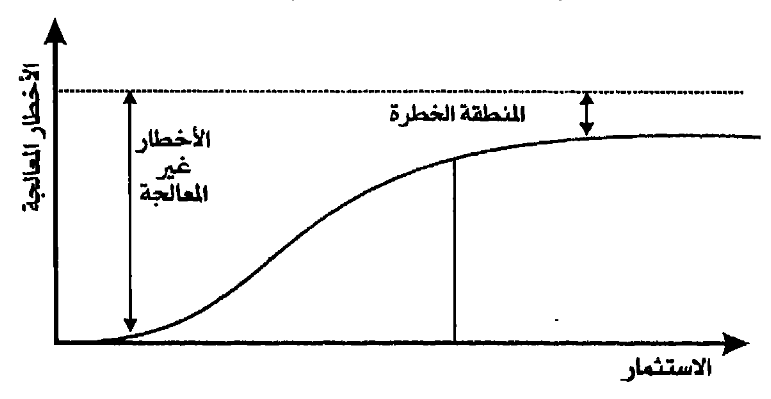
ويبين الشكل التالي (٥-١) تزايد الآثار المترتبة على الكارثة كلما ازداد حجم الكارثة، ويظهر جليًا تأثير وجود خطة لمواجهة الكوارث لدى المؤسسة، إذ نرى أنه في وجود الخطة لا تزيد الآثار المترتبة على الكارثة كثيرًا مع زيادة حجم الكارثة، بينما نجد أنه في غياب خطة مواجهة الكوارث فإن الآثار المترتبة على الكارثة تزيد بمعدل كبير مع ازدياد حجم الكارثة.



شكل (٥-١) تغير الآثار المترتبة على الكارثة مع تغير حجمها

كما يبين الشكل التالي (٥-٢) أهمية زيادة الإنفاق على نشاط معالجة

الأخطار، فيبين الشكل كيف أنه كلما زادت الاستثمارات المرصودة لنشاط معالجة الأخطار أدى ذلك إلى زيادة كمية الأخطار المعالجة، ومن ثم تقليل فرص المخاطرة أي تحسين أمن النظام، ونلاحظ أن المنحنى يصل إلى مرحلة الثبات في النهاية مهما زادت المبالغ المستثمرة، مما يعني أننا لا نستطيع أن نصل إلى معالجة كاملة (١٠٠ %) للمخاطر ولكن الهدف هو جعل المنطقة الخطرة (المخاطر غير المعالجة) أقل ما يمكن.



شكل (٥-٢) معالجة الأخطار(Risk management)

٢-٢- الوعي بأهمية التخطيط لمواجهة الكوارث

لكي نوضح درجة الوعي بالأمن لدى المؤسسات في العالم يمكن اللجوء إلى الدراسة التي أجريت على الشركات في بعض الدول الاسكندنافية [Daler 1989] والتي أظهرت أن:

١) ٢٣% من الشركات لا تستطيع الاستمرار في أداء أعمالها بدون خدمات الحاسب الآلي ولو لفترة قصيرة (يوم واحد أو يومان).

٢) ٤١% من هذه الشركات يمكنها الاستمرار في العمل بدون خدمات الحاسب الآلي ولكن لمدة يوم أو يومين.

٣) ٢٩% من الشركات ليست لديها أية إجراءات أمنية أو خطط طوارئ تساعد على استعادة القدرة على الأداء في حالات الكوارث.
٤) ٢٦% منها لم توقع أي اتفاق مع مركز بديل لضمان استمرار الأداء في حالة الكوارث.

٣- الأخطار المحتملة والمسببة للكوارث

٣-١- ما هو الخطر؟

الخطر (Threat) ،إذا كنا نتحدث عن أمن المعلومات، يقصد به أي ظرف أو حادث يحتمل أن ينتج عنه أذى لأحد النظم أو الأنشطة في شكل إفشاء للمعلومات أو تعديلها أو فقدها أو تدميرها. وهكذا فالخطر هو مجرد احتمال حدوث الأذى برغم أن وجود الخطر لا يعني ضرورة وقوع الأذى. واحتمال حدوث الخطر قائم دائمًا، وهو ينشأ لمجرد وجود النظم أو الأجهزة وليس لضعف معين فيها، فخطر اندلاع النيران مثلاً هو خطر قائم مهما كانت الاحتياطات المتخذة للوقاية منها.

لابد من عمل دراسة وافية لمحيط العمل وطبيعته ولنوع المعدات المستخدمة في نظام المعلومات وطريقة توزيع الأجهزة في صالة التشغيل وفي المؤسسة بصفة عامة، وكذلك دراسة شبكات نقل البيانات ، والبرمجيات المستخدمة ونظام التشغيل وبرامج أمن المعلومات في حالة توافرها، ودراسة تدفق البيانات خلال إدارات المؤسسة، وكيفية تبادل البيانات بين المؤسسة والجهات الخارجية، ودراسة درجة تأمين النظام ككل، وذلك بهدف تحديد نقاط الضعف في النظام لتحديد احتمالات الأخطار والكيفية التي ربما تحدث بها الجرائم ومن الذي يُخشى منه ارتكابها؟ وأين يمكن أن تقع هذه الجرائم؟

٣-٢- مكامن الخطر

الشكل (٥-٣) مكامن الخطر في المؤسسة



انهيار النظام

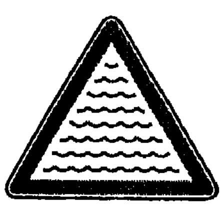

سرقة البيانات


التجسس


الحريـق

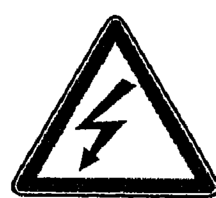

حادث عفوي


تزويـر

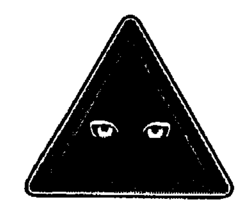

فيضـان


تخريـب


انقطاع الاتصالات الهاتفية

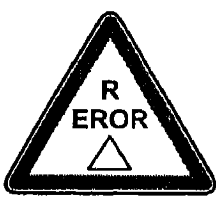

الصواعق


دخول غير مشروع


انقطاع الكهرباء


مخاطر مجهولة


الفيروسـات



أخطاء الإدخـال


الانفجـارات

٤- المبادئ الأساسية لنجاح نشاط مواجهة الكوارث

إن المبادئ الأساسية التي تمنح نشاط مواجهة الكوارث فرصة طيبة للنجاح وتحقيق الهدف منه يمكن تلخيصها في خمس نقاط هي:

٤-١- الحصول على التزام الإدارة العليا

بدون التزام الإدارة العليا الواضح والمعلن للجميع لن تكون هناك لهذا النشاط أي فرصة حقيقية للنجاح، فالإدارة العليا هي التي توفر الدعم المالي ودعمها المعلن لهذا النشاط هو الذي سيشجع الإدارات الأخرى على الاهتمام بما تكلف به من أنشطة أو دراسات أو ما يطلب منها من بيانات أو من مشاركة من جانب أفرادها في اللجان المختلفة، ولذلك نحرص دائمًا على أن يكون قرار الإدارة العليا بالموافقة على الخطة واعتماد المبالغ اللازمة لها هو أول صفحة في ملف خطة الطوارئ كما سنوضح عند الحديث عن ملف خطة الطوارئ.

٤-٢- توفير الميزانية اللازمة

نشاط مواجهة الكوارث، كأي نشاط آخر من أنشطة المؤسسة لابد وأن يحتاج إلى نفقات، ومن ثم لابد من توفير الميزانية اللازمة له مسبقًا، ولذلك كان من الضروري تقدير المبالغ المطلوبة في وقت مبكر. ومن طبيعة هذا النشاط أن المبالغ التي يتم رصدها لاستخدامها في حالات الطوارئ قد لا تستخدم في نفس السنة ولذلك لابد من اتخاذ الإجراءات اللازمة لترحيل هذه المبالغ من عام إلى آخر تحسبًا لحدوث الكارثة.

٤-٣- إيجاد موقع تشغيل بديل

البديل الاحتياطي، والذي سوف نتعرض له بالتفصيل في الفصل القادم، نعني به موقع التشغيل البديل الذي ينبغي إعداده للاستخدام عند تعطل الموقع الأصلي عن العمل. ولذلك لابد من الاهتمام بتجهيز هذا الموقع بدرجة الاستعداد المطلوبة، وكذلك معرفة المدة التي سوف يستغرقها إعداد الموقع بالكامل لاستقبال الموظفين والعملاء.

٤-٤- إجراء اختبارات استعادة النشاط باستمرار

نحن نعيش في عالم متغير، فكافة الظروف من حولنا قابلة للتغيير، ولذلك فمن الضروري ليس فقط إجراء الاختبارات اللازمة للتأكد من سلامة خطة استعادة النشاط ومن أنها سوف تؤدي الغرض منها، ولكن من المهم إعادة هذه الاختبارات على فترات دورية أو كلما ظهر متغير جديد نتوقع أن يكون له تأثير على الظروف العامة للمنشأة أو للموقع البديل. فربما نكتشف مثلاً إقامة محطة بنزين أو مستودع وقود بجوار المنشأة، أو قد تبدأ أعمال حفر بجوار الموقع البديل تعوق حركة إدخال الأجهزة إليه عند الحاجة إلى ذلك وقت الكارثة لا قدر الله. هذه المتغيرات كلها يمكن أن تؤثر كثيرًا على إجراءات استعادة النشاط وقد تتطلب منا إجراءات إضافية، لأن من المؤكد أننا لا نرغب في أن نفاجأ بمثل هذه الأمور في وقت نكون أحوج لكل دقيقة فيه.

٤-٥- إعداد خطة طوارئ ناجحة

خطة الطوارئ هي عصب نشاط مواجهة الكوارث، وإعداد خطة ناجحة يكفل نجاح هذا النشاط، ولذلك أفردنا الفصلين السابع والثامن بأكملهما لهذا الغرض، بالإضافة إلى عرض مثال لتطبيق خطة طوارئ مقترحة كملحق لهذا الكتاب.

الفصل السادس

تحليل المخاطر

موضوعات الفصل:

١- منهجية تحليل المخاطر.
٢- تقييم أصول المؤسسة.
٣- إدارة الأخطار.
٤- تقدير الخسائر المتوقعة.
٥- تحليل الأنظمة الحرجة.
٦- إجراءات حماية الأصول.
٧- البدائل الاحتياطية.



خصصنا هذا الفصل للحديث عن تحليل المخاطر التي تتعرض لها مراكز الحاسبات الآلية، فنقترح في بداية الفصل منهجية جديدة أكثر شمولاً لتحليل المخاطر تستفيد من الأعمال السابقة في هذا المجال، ثم نتحدث عن مراحل المنهجية المقترحة بالتفصيل، فنبدأ بالمرحلة الأولى وهي مرحلة تحديد وتقييم أصول المؤسسة مع إعطاء الأمثلة لذلك، ثم المرحلة الثانية وهي إدارة الأخطار بما في ذلك حصرها وتحديد درجة تعرض المؤسسة لها، ثم المرحلة الثالثة وهي تقدير الخسائر المتوقعة في حالة حدوث الكارثة ، لا قدر الله، ثم نتحدث عن المرحلة الرابعة التي تتعرض للأنظمة الحرجة وكيف نستطيع تحديد هذه الأنظمة من أجل أن نهتم بها دون غيرها في وقت الأزمة، وإعطاء مثال عملي لذلك، ثم نتحدث عن المرحلة الخامسة من المنهجية وهي إجراءات حماية الأصول، ثم ننهي الفصل بالحديث عن المرحلة الأخيرة من المنهجية المقترحة وهي البدائل الاحتياطية ومستوياتها المختلفة.

١- منهجية تحليل المخاطر

١-١- تحليل المخاطر (Risk Analysis)

المخاطرة هي الرهان على احتمال الحصول على عائد ما في المستقبل، وفي مجال الأعمال فالشيء الذي تتم المخاطرة به هو فقدان دخل محقق أو محتمل أو فقدان سمعة أو فقدان أي أصل آخر من الأصول . وبلغة رجال الأعمال فإن كل ذلك يترجم في النهاية إلى مبالغ مالية. والناس يقبلون بالمخاطرة عندما يتصورون أن هناك فرصة معقولة **ألا تحدث** النتائج غير المرضية.

وتحليل المخاطر هو مفهوم شائع في مجال الأعمال تمامًا مثلما هو شائع في حياتنا اليومية، فهو الإجابة عن التساؤل البسيط التالي: كم عليَّ أن أدفع الآن لتقليل إمكانية حدوث واقعة فرضية في المستقبل ستكلفني الكثير إذا وقعت؟ وكذلك السؤال التالي: أي بديل من البدائل العديدة المطروحة هو الأفضل من أجل تقليل احتمالات حدوث الكارثة؟

وقد تتراوح المشكلة من مشكلة بسيطة مثل قرار إبقاء التأمين الشامل على سيارة قديمة أو إلغاؤه، ويتوقف ذلك على احتمالات إصابة السيارة في حادث، وقد تصل إلى مشكلة كبيرة مثل اتخاذ قرار بنقل مصنع كامل من دولة إلى دولة أخرى، ويتوقف ذلك مثلاً على احتمالات تعرض الدولة التي نفكر في نقل المصنع إليها لقلاقل سياسية في المستقبل. في الحالتين نحتاج إلى التخمين والفرق الوحيد هو في حجم المشكلة وعدد العوامل المتضاربة التي تؤثر على عملية التخمين وكمية المعلومات المتوافرة للقائم بالتخمين.

فتحليل المخاطر في مجال تقنية المعلومات هو التقنية المستخدمة لتقليل درجة تعرض مركز الحاسب أو شبكة المعلومات مثلاً للمخاطر المتنوعة، ويجب أن يتم تنفيذ هذا النشاط (تحليل المخاطر) خلال مرحلة تصميم أي نظام من نظم المعلومات، لأن إجراءات الأمن التي يتم تضمينها للنظام من البداية تكون أكثر فاعلية من تلك التي تضاف للنظام في مراحل لاحقة.

١-٢- لماذا يجب أن نقوم بتحليل المخاطر؟

تحتاج المؤسسات لتحليل المخاطر التي قد تتعرض لها للأسباب التالية:

١) تسليط الضوء على الأخطار التي تتعرض لها المؤسسة وتحديد حجم هذه الأخطار.

٢) تسليط الضوء على مدى تأثر العمل بفقدان نظم الحاسب الحرجة لمدة طويلة.

٣) تحديد الحد الأقصى الممكن قبوله للمدة التي تتعطل فيها النظم الحرجة.

٤) تحديد النظم الحرجة وترتيب أولويات استعادتها (أيها يلزم استعادته أولاً).

٥) تحديد الموارد الحرجة اللازمة لاستعادة النشاط.

٦) تحديد التكلفة التي ينبغي تحملها لضمان أمن المؤسسة.

٧) تحديد أفضل مستوى للأمن يمكن الحصول عليه بمستوى إنفاق معين.

٨) تحديد النقطة التي يصبح عندها الإنفاق من أجل الأمان أعلى من الحد المقبول.

٩) تحديد درجة الثقة بإجراءات الأمان المقترحة.

١٠) إعداد توصيات بكيفية التعامل مع الأخطار التي تم تحديدها على أن تتناسب هذه التوصيات مع حجم المؤسسة ومع أهمية النظم الحرجة.

١١) تقديم المعلومات الكافية للإدارة العليا ليصبح في مقدورها اختيار الإستراتيجية المناسبة لاستعادة النشاط وما إذا كان هناك مبرر للاشتراك في إحدى الجهات التجارية التي تقدم الخدمة الاحتياطية.

١٢) إعطاء مؤشر للإدارة العليا عن الإجراءات اللازم اتخاذها لحماية المؤسسة وتقليل احتمالات وقوع كارثة.

١٣) وفي النهاية مساعدة الإدارة العليا على الموازنة بين تكلفة الإجراءات الأمنية المقترحة وبين التقدير الواقعي لأثر المخاطرة.

١-٣- دورة تحليل المخاطر

تتضمن معظم منهجيات تحليل المخاطر الخطوات التالية فيما يسمى بدورة تحليل المخاطر:

١) تحديد أصول المؤسسة المتمثلة في موارد الحاسب جميعها.

٢) تقييم الأصول بتحديد أهمية كل أصل من هذه الأصول للمؤسسة.

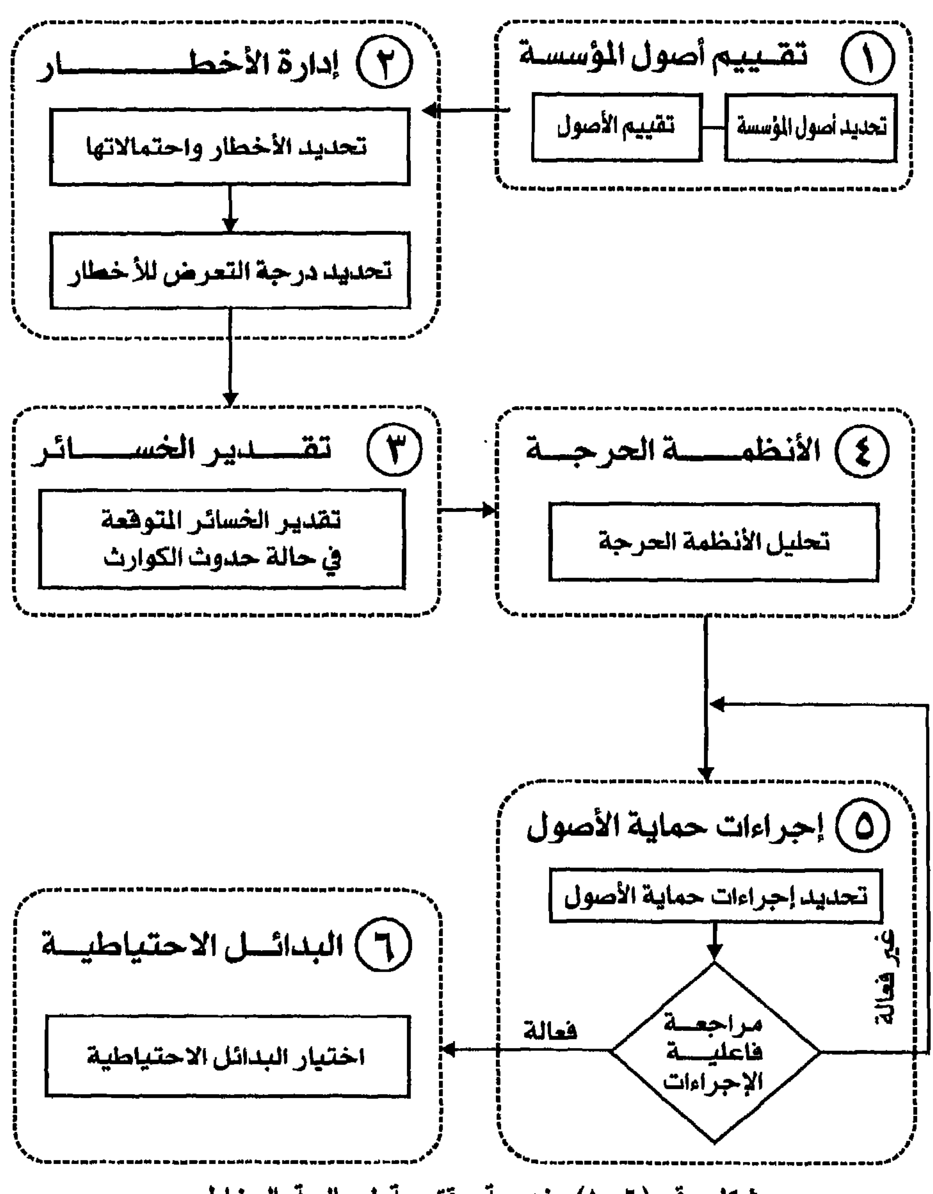
٣) تحديد الأخطار واحتمالاتها وتقرير حد المخاطرة المقبول لدى المؤسسة.

٤) اختيار إجراءات التأمين التي تقلل المخاطرة إلى الحد المطلوب.

٥) مراجعة فعالية الإجراءات المتخذة والتأكد من نجاحها.

١-٤- منهجية جديدة لمعالجة المخاطر

نقترح في هذا الكتاب منهجية أكثر شمولاً لمعالجة المخاطر تم بناؤها بضم الخطوات التي تشملها معظم منهجيات تحليل المخاطر مع دراسة الأنظمة الحساسة في المؤسسة وتحليلها، ثم وضع الخطوات اللازمة لتحييد الأخطار التي تتعرض لها المنشأة والتقليل من أثرها، وبعد ذلك تحديد البدائل الاحتياطية التي يمكن أن تلجأ إليها المؤسسة.



شكل رقم (٦-١) منهجية مقترحة لمعالجة المخاطر

ويبين الشكل (٦-١) منهجية معالجة المخاطر المقترحـــة فـــي هـــذا الكتاب. ويُراعى لنجاح تطبيق هذه المنهجية أن تتم مراجعة فعالية الإجراءات باستمرار نظرًا لتغير الكثير من العوامل التي بنيت عليها هذه الإجـــراءات، فبمرور الوقت تتغير قائمة الأصول وقيمة هذه الأصول. وبعد التوصل إلـــى منظومة إجراءات الأمن المبينة بالشكل (٦-١) يصبح إدخال التعديلات عليها سهلاً عند إضافة أصول جديدة إلى المؤسسة كأجهزة أو برامج، وبالتـــالي لا نحتاج إلى إعادة عملية التحليل بالكامل وإنما ندرس فقط أثر التغيـــير الـــذي حدث من إضافة أو حذف للأصول. ويلاحظ هنا أن نتـــائج عمليـــة تحليـــل المخاطر تعتبر في حد ذاتها من المعلومات عظيمة الأهمية للمؤسسة طالمـــا أنه تتم مراجعتها باستمرار، فتصبح بذلك أصلاً من أصول المؤسسة ويجـــب الحفاظ عليه.

يتضح لنا أن منهجية معالجة المخاطر المقترحة تتضمن الأنشطة التالية والتي سنتعرض لها بالتفصيل في هذا الفصل:

١) تقييم أصول المؤسسة

في هذا النشاط يتم حصر أصول المؤسسة وتقييمـــها وتحديـــد مـــدى أهميتها لنجاح العمل الرئيسي للمؤسسة.

٢) إدارة الأخطار

يتضمن هذا النشاط تحديد مصادر الخطر التي تـــهدد هـــذه الأصـــول وتقييم مدى خطورة هذه المصادر على أصول المؤسسة، ثم يتبع ذلك تحديـــد درجة التعرض للأخطار (Vulnerability) حيث يتم تحديد مـــدى ضعـــف النظام في مواجهة هذه الأخطار.

٣) تقدير الخسائر

في هذا النشاط يتم توقع الخسائر التي قد تُمنى بها المؤسسة في حالة حدوث الكارثة على اختلاف أنواع الكوارث المتوقعة.

٤) تحليل الأنظمة الحرجة

تتضمن هذه المرحلة تحديد الأنظمة الحرجة التي ينتج عن توقفها أن تتأثر بشدة الأهداف الرئيسية للمؤسسة.

٥) إجراءات حماية الأصول

في هذه المرحلة يتم تحديد الإجراءات المضادة التي يجب اتخاذها لحماية أصول المؤسسة كما يتم من آن لآخر مراجعة فعالية هذه الإجراءات وتعديلها إن لزم الأمر.

٦) البدائل الاحتياطية

في هذه المرحلة تتم المفاضلة بين البدائل المتاحة والتي يمكن استخدامها في حالة تعطل جهاز الحاسب عن العمل واختيار أحد هذه البدائل.

٢- تقييم أصول المؤسسة

٢-١- تحديد أصول المؤسسة

أصول المؤسسة هي ببساطة أي شيء ذو قيمة أو ذو فائدة، وهذه الأصول قد تكون مادية (كأجهزة الحاسب أو محطات تكييف الهواء أو توثيق البرامج) أو تكون برمجية (كنظام التشغيل أو البرمجيات العامة أو برامج التطبيقات في المؤسسة) وقد تكون الأصول هي البيانات (المعلومات) وهي

الأكثر أهمية. ولذلك يجب تحديد هذه الأصول في البداية، وفيما يلي بعض الإرشادات التي تساعد على تحديد الأصول :

١) في البداية يجب تحديد العتاد (H/W) بما في ذلك جميع أجهزة الحاسب (مهما كان حجمها) والطرفيات وأجهزة الإدخال والإخراج.

٢) تحديد البرمجيات (S/W) بما في ذلك برامج التشغيل والبرامج المساندة وبرامج التطبيقات سواء كانت مشتراة من خارج المؤسسة أو مطورة داخلها.

٣) تحديد الأصول المتصلة بنشاط الاتصالات بما في ذلك الأجهزة المستخدمة في الاتصال وأجهزة التحكم والكابلات بأنواعها.

٤) تحديد الخدمات الأساسية المهمة مثل: مبنى الحاسب ومكاتب موظفي الحاسب ولمن هي مخصصة إلى جانب خدمات الكهرباء والماء وأجهزة تكييف الهواء، وحتى الأدوات المكتبية. يدخل في هذه المجموعة كذلك توثيق النظام سواء التوثيق الورقي أو المحفوظ على الوسائط الممغنطة.

٥) تحديد البيانات ذات الأهمية بالنسبة للمؤسسة وهي إما تكون في ملفات منفصلة أو ضمن قواعد بيانات كبيرة، ويجب في كل حالة تسجيل المصدر الذي ترد منه هذه البيانات والجهة التي تستخدمها.

٢-٢- تقييم الأصول

١) لكل من الأصول الأربعة الأولى (العتاد والبرمجيات وأجهزة الاتصالات والخدمات الأساسية) يتم احتساب تكلفة استبدالها، والمقصود بذلك التكلفة التي ستتحملها المؤسسة لشراء بديل جاهز من السوق، وهو كما تقدم

أمر بسيط بالنسبة للأجهزة والبرمجيات المشتراة، أما بالنسبة لباقي الأصول فسيتطلب الأمر الكثير من التخمين.

أما فيما يتعلق بالأفراد أو المباني التاريخية مثلاً فقد يكون من المستحيل الوصول إلى قيمة دقيقة.

٢) بالنسبة للبيانات كأصل من أصول المؤسسة لا يمكن تحديد قيمة الاستبدال مثلما نفعل مع الأجهزة، ولكن تحتسب التكلفة التي تقع على المؤسسة إذا فُقدت هذه البيانات أو أتلفت أو أفشيت لغير ذي صلاحية أو تم تحويرها عفوًا أو عمدًا. في هذه المرحلة يمكن التوصل إلى رقم محدد يمثل الخسارة بالنسبة لكل نوع من أنواع فقد البيانات (فقد / إفشاء / تدمير/ تعديل) ، ويؤخذ أكبر هذه الأرقام (وليس مجموعها) وهو يمثل قيمة هذا الأصل من أصول البيانات.

إذا كان تقدير هذه الأرقام يشكل صعوبة بالنسبة للقائمين بتحديد قيمة الأصول ، فيمكن لتسهيل هذه المهمة تحديد وزن يمثل الأهمية لكل نتيجة من النتائج التالية المترتبة على فقد البيانات من وجهة نظر المؤسسة:

- الخسارة المالية.
- الخصوصية الفردية.
- النواحي القانونية.
- الأسرار التجارية.
- تعطيل المستفيدين.
- الحرج السياسي.
- سلامة الأفراد.

وهذا سيجعل عملية تقدير قيمة الأصول أكثر سهولة.

ويراعى هنا أن يقتصر التعامل مع بيانات الأنظمة الحرجة فقط وهي الأنظمة التي تمثل أهمية خاصة للمؤسسة وينشأ عن توقف العمل بها ضرر شديد للأهداف الرئيسية للمؤسسة، وسوف يخصص موضوع خاص في هذا الفصل لتوضيح كيفية تحديد هذه الأنظمة ، كما يتضمن ملحق الكتاب تطبيقًا لذلك. ويجب **دائمًا** أن نأخذ في الاعتبار **(أسوأ الاحتمالات)**، فنختار أسوأ أوقات العام أو الشهر لتوقع حدوث الكارثة إذا حاقت بالبيانات، فنحدد بذلك أعلى تكلفة للكارثة في جميع الأحوال.

٢-٣- مثال لعملية تقييم الأصول

يوضح المثال التالي المبين في الجدولين (٦-١) و (٦-٢) كيفية تقويم الأصول المستخدمة بإحدى المؤسسات التي تعتمد في المقام الأول على أجهزة الحاسب المركزي (Mainframe) بالإضافة إلى مجموعة من الشبكات المحلية التي تتواجد لدى إدارات المؤسسة ويتم ربطها من خلال (Gateway) وتستخدم الحاسبات الشخصية الموجودة في هذه الشبكة كطرفيات لإجراء العمليات المطلوبة على الحاسب المركزي. وتمت الاستعانة عند تقدير هذه الأصول بقسم الدعم الفني بالمؤسسة.

١) تقييم تكلفة تأثر الأصول المادية ونظم التشغيل بالكارثة:

نوع الأصل	القيمة	كيفية احتساب القيمة
الأصول المادية (العتاد):		تكاليف شراء بديل
• وحدة المعالجة المركزية CPU	١,٠٠٠,٠٠٠	
• وحدات تخزين DASD	٥٠٠,٠٠٠	
• أجهزة قراءة أشرطة	٢٠٠,٠٠٠	
• الطابعات	٢٥٠,٠٠٠	
• حاسبات شخصية	٢٠٠,٠٠٠	
الأصول المادية(أجهزة الاتصالات):		تكاليف شراء بديل
وحدات التحكم	٣٥٠,٠٠٠	
طرفيات	٤٠٠,٠٠٠	
مكونات الشبكات المحلية	٤٥٠,٠٠٠	
نظم التشغيل:		تكلفة إعادة تركيب
MVS	٣,٠٠٠	الأنظمة واختبارها
DB2	٣,٠٠٠	
ACF2	١,٠٠٠	
CICS	٢,٠٠٠	
Netware	١,٠٠٠	
الخدمات الأساسية	٣,٠٠٠,٠٠٠	تكلفة تقديرية إجمالية
الإجمالي	٦,٣٦٠,٠٠٠	

جدول رقم (٦-١): تقييم تكلفة تأثر الأصول المادية ونظم التشغيل بالكارثة

٢) تقييم تكلفة تأثر بيانات الأنظمة الحرجة بالكارثة:

النظام الحرج	فقد	إفشاء	تدمير	تزوير	أعلى تكلفة
متابعة الخطة الخمسية	١,٠٠٠,٠٠٠	٢,٠٠٠,٠٠٠	٥,٠٠٠	٥,٠٠٠	٢,٠٠٠,٠٠٠
تلبية احتياجات العملاء	٢,٥٠٠,٠٠٠	٥٠٠,٠٠٠	٥,٠٠٠	٩٠,٠٠٠	٢,٥٠٠,٠٠٠
الإجمالي					٤,٥٠٠,٠٠٠

جدول رقم (٦-٢): تقييم تكلفة تأثر بيانات الأنظمة الحرجة بالكارثة

أي أن إجمالي التكلفة المباشرة التي سوف تقع على المؤسسة نتيجة حدوث الكارثة هي ١٠,٨٦٠,٠٠٠ ريال سعودي (٦,٣٦٠,٠٠٠ + ٤,٥٠٠,٠٠٠).

ويتضمن ملحق الكتاب (خطة طوارئ مقترحة لمعهد الإدارة العامة) تقييمًا آخر لأصول معهد الإدارة العامة.

٣- إدارة الأخطار (Risk Management)

٣-١- تحديد الأخطار المحتملة

سنقوم فيما يلي بحصر أكثر الأماكن في المؤسسة عرضة للأخطار المحتملة:

٣-١-١- الأفراد:

- **مكامن الخطر** : إجراءات التعيين وإجراءات إنهاء الخدمة، حجم التدريب ومداه، نوعية الإشراف في كافة المستويات.
- **الأخطار المحتملة** : تعديل البيانات أو إخفاؤها، ارتكاب الأخطاء العفوية أو المتعمدة (التزوير) خلال إدخال البيانات، منح صلاحية الاستخدام لموظف ناقم على المؤسسة، الاختلاس، الإصابة أو الوفاة، استخدام موظف للبيانات بعد تركه الخدمة، انتهاك الخصوصية، الإضراب، السرقة، إفشاء البيانات لغير المختصين.

٣-١-٢- بيئة الحاسب:

- **مكامن الخطر** : الأماكن والأبنية المجاورة للمؤسسة، نوعية وكفاءة الخدمات كالكهرباء والمياه والمجاري ، تصميم المبنى نفسه، التشغيل والصيانة، ضوابط الدخول المادية.
- **الأخطار المحتملة** : ذرات الغبار، تعطل أجهزة التكييف، الزلازل، الانفجارات، الحريق (سواء كان محدودًا أو ضخمًا، خارجيًا أو داخليًا)، الفيضان، الأعاصير، العواصف الثلجية أو الترابية، الثورات البركانية، الانهيارات الأرضية، الصواعق، تسرب المياه، تعطل الإمداد بالطاقة الكهربية، تفريغ الشحنات الكهربية الإستاتيكية، الشغب، الأعمال الإرهابية، دخول أفراد غير مختصين إلى المبنى.

٣-١-٣- المعدات والبرمجيات:

- **مكامن الخطر** : صلاحيتها للعمل ، الإجراءات التي تنظم إدخال

التعديلات عليها، مطابقتها للمواصفات، التوثيق.

- **الأخطار المحتملة :** العبث بالأجهزة، تعطيل الأجهزة، سوء أداء الأجهزة أو البرمجيات، تعديل البرمجيات، تعطيل البرمجيات، تعديلات نظام التشغيل أو الأخطاء فيه.

٣-١-٤- أجهزة الاتصالات:

- **مكامن الخطر :** الأجهزة ودوائر نقل البيانات، الإجراءات المتبعة للتحقق وتنظيم توزيع الرسائل.
- **الأخطار المحتملة :** أعطال الاتصالات، الانقطاع الكامل للاتصال، التنصت، ثقب الكوابل (Wire Tapping) ، التداخل الكهرومغناطيسي، إعاقة موجات البث، إقحام رسائل غريبة في الخطوط أو حذف بعض الرسائل المتبادلة، التخريب المتعمد.

٣-١-٥- نظم التطبيقات:

- **مكامن الخطر :** التصميم الفني للنظم، معايير التوثيق، ومعايير الجودة.
- **الأخطار المحتملة :** عدم كفاية الاختبارات على النظام، أخطاء البرمجة، التعديلات غير المرخص بها، تدمير الملفات.

٣-١-٦- تداول موارد الحاسب:

- **مكامن الخطر :** الإجراءات والمعايير المتبعة لحماية أصول البرامج، التحكم في الإدخال والإخراج، أنواع مكتبات الأشرطة، العمليات التي تتم في صالة الحاسب، الصيانة الدورية، توزيع الأجهزة والأثاث في صالة الحاسب.

- **الأخطار المحتملة** : سوء تداول البيانات أو الوسائط التي تحتويها، التجسس، تسريب المعلومات وإفشاؤها.

٣-٢- درجة التعرض للأخطار (Vulnerability)

درجة التعرض (Vulnerability) لا نعني بها احتمال حدوث الخطر وإنما هي درجة الضعف أو الخلل في نظام معلومات والذي يمكن أن يُستغل ليسبب ضرراً للنظام، وكلما زادت درجة التعرض للخطر زاد تأثير الخطر على الأصول عند وقوعه، ومقياسها هو احتمال نجاح الخطر إذا وقع في إلحاق الضرر بالنظام. وبعبارة أخرى فهي العلاقة ثلاثية الأبعاد بين الضرر المتوقع والأصل المعرض للخطر والخطر نفسه ، ولنأخذ في الاعتبار الأمثلة التالية:

١) فقد توثيق برنامج الصيانة بسبب السرقة هو ضرر يحدث نتيجة ضعف ضوابط الاستخدام. فالفقد هنا هو الضرر الذي وقع، وتوثيق البرنامج الذي فقد هو الأصل المعرض للخطر، والسرقة هي الخطر ذاته، وضعف ضوابط الاستخدام هي درجة التعرض (Vulnerability).

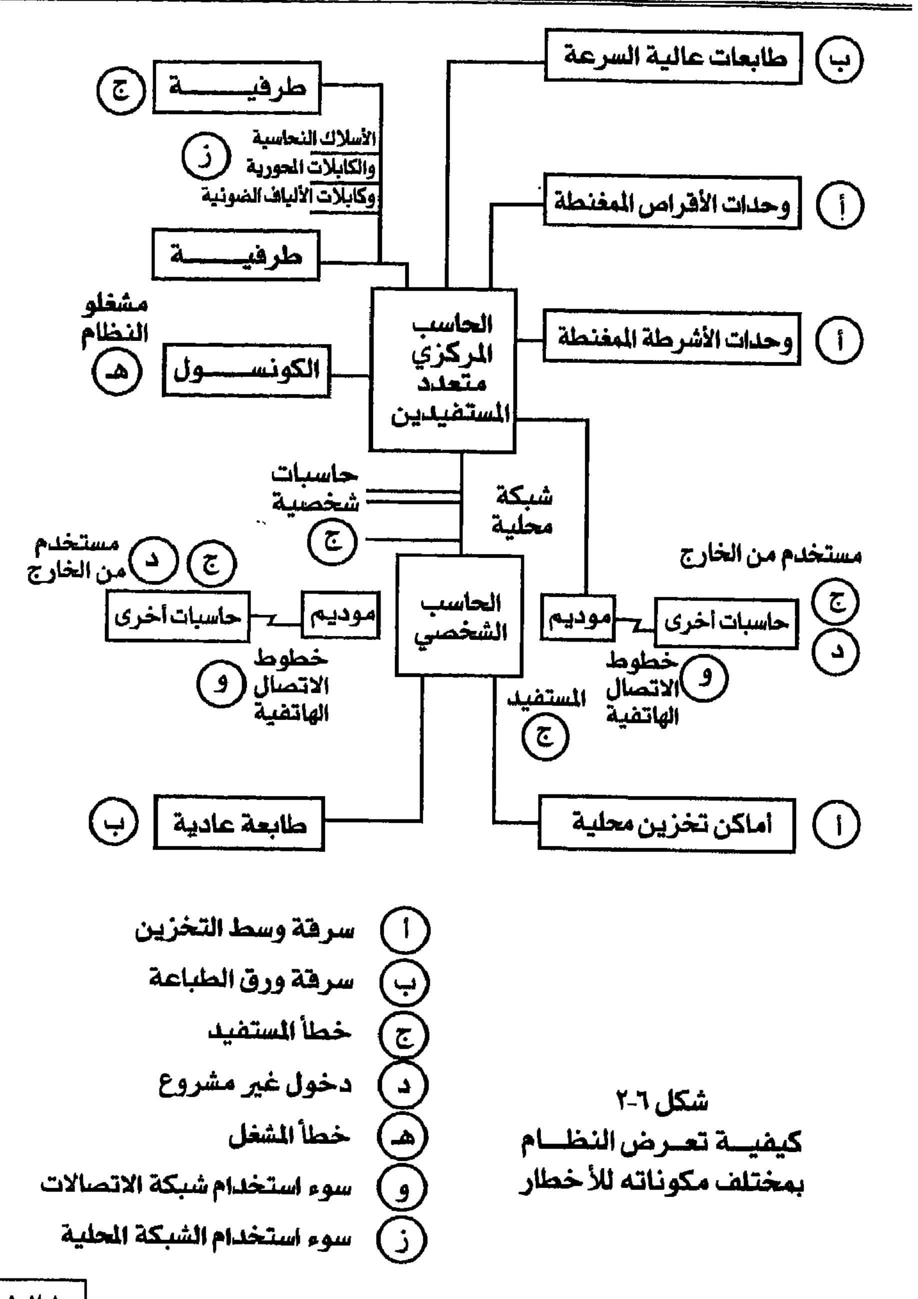
٢) تعديل الرصيد في حساب بأحد البنوك عن طريق تدخل غير مشروع لتنفيذ معاملة إضافة إلى الحساب هو ضرر يحدث نتيجة الافتقار إلى ضوابط تأمين مرور الرسائل في الشبكة. فتعديل الرصيد هنا هو الضرر الذي وقع، والحساب المصرفي هو الأصل المعرض للخطر،

والتدخل غير المشروع هو الخطر، أما الافتقار إلى ضوابط تأمين مرور الرسائل في الشبكة فهو درجة التعرض.

٣) فقد أشرطة النسخ الاحتياطي لقاعدة البيانات الخاصة بنظام المخازن في حادثة حريق هو ضرر يحدث نتيجة عــدم كفايــة خطــط الطــوارئ. فالضرر هنا هو فقد الأشرطة، وأشرطة النسخ الاحتياطي وربما قــاعدة البيانات نفسها هي الأصل المعرض للخطر، والخطر بالطبع يتمثل فــي الحريق، أما درجة التعرض فهي عدم كفاية خطط الطوارئ.

من أجل حساب درجة التعرض بشكل دقيق يجب فحـــص الأصـــول ومكامن الخطر في المؤسسة وإجراء المقابلات مع المديرين والموظفين الذين هم على دراية بالإجراءات والعمليات اليومية التي تنفذ بالمؤسسة، ومن خلال هذه الفحوص والمقابلات يتم تســجيل كــل احتمــالات التعــرض للخطــر بالتفصيل، فإذا ثبت أن درجة تعرض المؤسسة (Vulnerability) كبيرة فيما يتعلق بالأخطار التي سبق تحديدها في مرحلة تحديد الأخطار المحتملة فيجب اتخاذ الإجراءات المضادة المناسبة لحماية أصول المؤسسة وهو مــا نطلــق عليه إدارة الأخطار وتقليل أثرها (Risk management) .

ويبين الشكل (٦-٢) كيفية تعرض النظام بمختلف مكوناته للأخطار:



شكل ٦-٢
كيفيـــة تعـــرض النظـــام
بمختلف مكوناته للأخطار

٣-٣- مثال عن تحديد الأخطار التي تتعرض لها الأصول

٣-٣-١- نسبة التعرض للخطر:

الأخطار / الأصول	الحريق	السرقة	التلف	الإتلاف العمد	الكوارث الطبيعية (*)
الأصول المادية (العتاد):					
وحدة المعالجة المركزية CPU	%٥	%٠,٥	%١٠	%١	%٠,٥
وحدات تخزين DASD	%٥	%٠,٥	%١٥	%١	%٠,٥
أجهزة قراءة أشرطة	%٥	%٠,٥	%١٨	%١	%٠,٥
الطابعات	%١٠	%٢	%٢٠	%١	%٠,٥
حاسبات شخصية	%٢	%١٠	%٥	%٢	%٠,٥
الأصول المادية(أجهزة الاتصالات):					
وحدات التحكم	%٥	%٠,٥	%١٠	%١	%٠,٥
طرفيات	%٢	%١٠	%٢	%١	%٠,٥
مكونات الشبكات المحلية	%٣	%٥	%١٠	%٢	%٠,٥
نظم التشغيل:					
نظام MVS	-	%٠,٥	%٤	%٢	%٠,٥
نظام DB2	-	%٠,٥	%٤	%٢	%٠,٥
نظام ACF2	-	%٠,٥	%٤	%٢	%٠,٥
نظام CICS	-	%٠,٥	%٤	%٢	%٠,٥
نظام Netware	-	%٠,٥	%٤	%٢	%٠,٥
الخدمات الأساسية	%٥	%١٠	%١٠	%٢	%٠,٥

الأصول / الأخطار	سرقة	إفشاء	تدمير	تزوير
ملفات النظم الحرجة:				
نظام متابعة الخطة الخمسية	%٥	%١٠	%١٠	%٢
نظام تلبية احتياجات العملاء	%٥	%١٠	%١٠	%٢

(*)الكوارث الطبيعية تشمل: الصواعق ، الزلازل ، البراكين ، والفيضانات ... الخ

جدول رقم (٦-٣): تعرض أصول مركز الحاسب الآلي للأخطار

يبين الجدول (٦-٣) مثالاً عن نسبة تعرض أصول مركز الحاسب الآلي للأخطار.

٣-٣-٢- مثال لدراسة درجة التعرض للأخطار لمركز حاسب آلي

١) أمن المنشأة:

يقع مركز المعلومات في نفس المجمع الذي تقع فيه باقي إدارات المؤسسة، ولكن في مبنى مستقل يتكون من دورين. يتميز الموقع ببعده عن الأخطار البيئية المحتملة كبعده عن خزانات الوقود والمياه كما أن غرفة التشغيل تقع في الدور الأرضي ونوافذها مسيجة، أما مكاتب الموظفين فتقع في الدور الأول مما يضمن عزل مناطق العمل عن بعضها البعض. تستخدم البطاقات الممغنطة للدخول إلى المركز بالإضافة إلى وجود حارس أمن على مدار الساعة، ويلتزم الموظفون بتعليق بطاقات إثبات شخصية خلال تواجدهم بالمبنى. ولكن لوحظ أنه لا تستخدم بطاقات تعريف للزائرين.

٢) أمن غرفة الحاسب الآلي :

غرفة الحاسب الآلي معزولة عن باقي المكاتب ويتم الدخول إليها باستخدام البطاقات الممغنطة. وتعمل ثلاث ورديات للتشغيل على مدار الساعة بحيث يتواجد اثنان من المشغلين على الأقل في الغرفة. ولكن لوحظ أن هناك عدداً من "الكوابل" في أرضية الغرفة لم يتم عزلها.

٣) وسائل الرقابة ضد الحريق :

التدخين ممنوع في جميع مرافق وغرف المبنى، كما توجد صيانة دورية كل ثلاثة أشهر لأجهزة التكييف ولأجهزة الإطفاء الآلية، حيث توجد بالغرفة أجهزة إنذار بالحريق، كما يستخدم غاز الهالون لإطفاء الحرائق آليًا. ويتم اختبار وسائل اكتشاف الحريق والإنذار به وجميع الأجهزة المساندة بشكل دوري. أما من حيث التأمين ضد الحريق فإن عقد التشغيل والصيانة ينص على التزام شركة التشغيل بإيجاد مركز بديل في حال حدوث كارثة.

ولكن لوحظ أنه لم تستخدم الأصباغ المقاومة للحرائق في المبنى بشكل عام، كما وجد أن الأسقف المستعارة المستخدمة غير مقاومة للاشتعال، ووجد أنه من الأفضل استخدام مادة (MS40) بدلاً من غاز الهالون المستخدم حالياً.

٤) الخدمات الأساسية المساندة :

يستخدم مركز الحاسب مصدر الإمداد بالطاقة (UPS) بحيث تعمل البطاريات الخاصة به لمدة ساعة، بالإضافة إلى وجود مولدات احتياطية لتوليد الكهرباء في مبنى مجاور، وهناك عقد صيانة يتجدد سنويًا لصيانة هذه الأجهزة لضمان استمرارية عملها.

٥) الاتصالات التليفونية :

يتم استخدام خطوط هاتفية مؤجرة (Leased lines) بالإضافة إلى وجود خطوط احتياطية، وهي خطوط "مراقمة" (Dial up) ، كما يوجد بالمركز أجهزة مودم احتياطية وأجهزة بديلة للأجهزة المساندة الأخرى بما يضمن استمرار عمل الفروع.

٦) وظيفة ضابط أمن نظم المعلومات :

يوجد قسم خاص لأمن نظم المعلومات يعمل به ثلاثة أفراد ويرأسهم مهندس نظم معلومات، وتلقى جميع الموظفين تدريبًا في مجال أمن المعلومات، ولكن لوحظ أن القسم لم يقم بعد بإعداد خطة للطوارئ.

٣-٤- أسباب زيادة تعريض النظام للخطر

ونورد فيما يلي حصرًا للأسباب التي تزيد من درجة تعرض أي نظام للأخطار:

١) عدم دعم الإدارة العليا لأمن الحاسب.

٢) عدم فعالية الإجراءات الأمنية المتخذة.

٣) عدم كفاية تدريب وتوعية الموظفين في مجال الأمن.
٤) عدم ولاء بعض الموظفين.
٥) عدم فعالية إجراءات إدارة الأخطار في المؤسسة.
٦) عدم كفاءة وسائل التأمين كطفايات الحريق.
٧) عدم كفاية إجراءات الرقابة والمراجعة.
٨) إذا كان نظام التحكم في استخدام الوثائق غير آمن.
٩) إذا كانت إجراءات استعادة النشاط غير آمنة.
١٠) عدم فعالية أساليب اكتشاف الخطأ في النظم.
١١) إذا كانت عملية تطوير التطبيقات غير آمنة.
١٢) إذا كانت صيانة النظم والتطبيقات غير آمنة.
١٣) إذا كانت إجراءات قبول البرمجيات غير آمنة.
١٤) إذا كانت خطة الطوارئ غير شاملة.
١٥) إذا كان نظام الاتصالات غير آمن أو غير موثوق به.
١٦) إذا كانت إجراءات الإدخال والإخراج غير آمنة.
١٧) عدم فعالية ضوابط دخول الأفراد.
١٨) عدم كفاية ضوابط استخدام الطرفيات والنظام ككل.

٤- تقدير الخسائر المتوقعة

> **ربما كانت المعلومات هي أثمن الموارد في هذا العصر إلا أنها أكثر هذه الموارد تعرضًا للخطر في مجال الأعمال الحديث.**

٤-١- تصنيف الخسائر المتوقعة

لابد من التقدير المسبق للخسائر المتوقعة في حالة حدوث الكوارث حتى يمكن تبرير الإنفاق على الوقاية من هذه الكوارث، وتستخدم في هذا التقدير البيانات التاريخية وسجلات الحوادث المماثلة السابقة.

يمكن حصر الخسائر الرئيسية المترتبة على الكوارث بالنسبة لأي مؤسسة فيما يلي:

٤-١-١- خسائر مالية مباشرة:

- تدمير المعدات والتسهيلات.
- فقد المبيعات.
- فقد الإنتاج.

٤-١-٢- خسائر مالية غير مباشرة:

- فقد العملاء على المدى البعيد.
- دفع أجور إضافية للموظفين.

- عدم تحصيل مستحقات للمؤسسة لدى الغير.
- عدم اكتشاف التزوير.
- دفع غرامات تأخير.
- دفع غرامات عن بضائع تالفة.

٤-١-٣- فقد السيطرة:

- تأثر سلامة وتكامل البيانات.
- اتخاذ قرارات خاطئة في توجيه العمل.

٤-١-٤- إحراج المؤسسة:

- التعرض لهجوم وسائل الإعلام.
- إضعاف الصورة العامة للمؤسسة.

٤-٢- الأضرار التي تصيب المعلومات

إذا ركزنا على مجال تقنية المعلومات فإننا نستطيع أن نحدد ثلاثة أنواع من الضرر الذي يمكن أن يحدث للمعلومات وهي:

١) تأثر سلامة وتكامل البيانات:

وينتج ذلك عن التعديل أو الإتلاف (المتعمد أو غير المتعمد) لبيانات المؤسسة بأي شكل من أشكال تهديد البيانات التي ذكرناها سابقاً.

٢) انتهاك سرية البيانات:

وينتج ذلك عن الإفشاء (المتعمد أو غير المتعمد) للمعلومات.

٣) تعطل أي مكون من مكونات النظام:

ويكون هذا التعطل عن العمل إما مؤقتاً أو بصفة نهائية.

٤-٣- التقييم المالي للخسائر المتوقعة

في الحقيقة فإن تقدير الخسائر المتوقعة وتقويمها في صورة مبالغ مالية ليس بالأمر السهل، ولعل أسهل الخسائر التي يمكن تقديرها هي تلك التي تنتج عن تلف دائم للأصول مثل أجهزة الحاسب مما يستوجب إعادة شرائها، وربما احتاج الأمر إلى تأجير بديل لفترة زمنية معينة، وفي هذه الحالة تضاف قيمة التأجير إلى قيمة شراء المعدات عند حساب الخسارة الإجمالية. وهناك كذلك أجور العمالة المطلوبة لاستعادة البيانات من النسخ الاحتياطية، وتكلفة العمالة اللازمة لإعادة تركيب البرمجيات والنظم التطبيقية على الأجهزة البديلة، وكذلك تكلفة استقدام مستشارين من خارج المؤسسة لتقديم المشورة حول استعادة النشاط، هذا إلى جانب التكلفة المباشرة للعمالة المطلوبة لتركيب الأجهزة الجديدة.

أما الخسائر غير المباشرة المترتبة على الكارثة فهي كثيرة ومتنوعة فهناك الوقت المهدر دون إنتاج سواء بالنسبة لنظم الحاسب أو بالنسبة للأعمال الرئيسية للمؤسسة التي تعتمد على هذه النظم، إذ إن جميع نظم الحاسب في المؤسسات الحديثة الآن تعتبر من العوامل الحرجة بالنسبة للعمل (Business Critical) فإذا تعطلت تأثر العمل بشدة، وهناك أيضًا الوقت الذي يتوقف فيه تطوير البرامج بسبب توقف خدمات الحاسب، وهناك كذلك وقت المديرين الذي ينفق لمتابعة الكارثة واستعادة النشاط، والوقت الذي ينفق لتقويم أثر الكارثة على العمل ككل ولاتخاذ الإجراءات اللازمة لتجاوز المشكلة، ولذلك فحتى إذا تم تجاوز المشكلة بنجاح وعادت الأمور إلى مجاريها، فإن ذلك لن يتم إلا بالكثير من الوقت والجهد الذي ينفقه المديرون في المؤسسة على جميع المستويات.

أما الخسارة الحقيقية فهي التي تتمثل في فقدان الثقة بالمؤسسة ، وربما كانت هذه هي أهم النتائج المترتبة على وقوع الكارثة، فالثقة التي يُخشى

فقدها هي ثقة العملاء والشركات الموردة، وثقة الموظفين وحملة الأسهم والمؤسسات الأخرى التي ترتبط أعمالها بأعمال المؤسسة، فتجد هؤلاء جميعًا يرقبون الوضع بقلق للتأكد من قدرة المؤسسة على تجاوز المحنة والتأكد من أنها سوف تستطيع الوفاء بالتزاماتها.

وتبدأ التكلفة الناتجة عن الخسارة في التصاعد (وربما التسارع) إذا تدخلت في الأمر بعض العوامل المسببة لتأخير استعادة النشاط، مثل عدم توافر بعض المواد الحرجة الذي قد يمنع تنفيذ إجراءات استعادة النشاط التي أُعدت سلفًا بالاعتماد على وجود هذه الموارد، أو مثل غياب بعض تسهيلات الاتصالات أو تأخر الإمداد الكافي بوسائط التخزين المؤقتة، أو عدم توافر الأفراد المدربين، أو عدم التوافق بين البرمجيات التي استخدمت في إعداد النسخ الاحتياطية قبل الكارثة مع بيئة الحاسب الجديدة مما يمنع استعادة البيانات، أو الافتقار إلى التخطيط والإعداد الكافيين، فالحصول على الأجهزة والمعدات لا يشكل مشكلة في معظم الأحوال ويمكن الحصول عليه بسرعة نسبيًا إلا أن هذه المعوقات التي ذكرناها هي التي تسبب المشكلات.

ولا تستغني أي مؤسسة عند إعداد خطة الطوارئ الخاصة بها عن تقدير الأخطار (Risk Assessment) والذي يتضمن أولاً تحديد احتمالات وقوع الكارثة ، ثم حساب التكلفة المادية التي تقع على المؤسسة نتيجة لوقوع الكارثة، ويكون الناتج من عملية تقدير الأخطار تحديد مبلغ معين (بالريالات مثلاً)، ويتم ذلك عن طريق حساب "الخسارة السنوية المتوقعة" (خ س م) (Annual Loss Expectancy A L E) التي تحدد بضرب معدل حدوث الكارثة (م) أي عدد مرات حدوثها في السنة × الخسارة المتوقعة (خ) في كل مرة تحدث فيها الكارثة، أي:

$$خ س م = م \times خ$$

فإذا أخذنا مثلاً كارثة الحريق في أحد مراكز الحاسب الآلي واحتمال

حدوثه (بناء على استقراء الإحصائيات) هو مرة كـــل ٢٠٠٠ ســنة أي أن الاحتمال السنوي لحدوثه أي معدل حدوث الكارثة (م) هو ٠,٠٠٠٥ وقيمــة الخسارة المتوقعة إذا وقع هذا الحادث (خ) هي عشرة ملايين ريال. وبذلــك تكون الخسارة السنوية المتوقعة كالتالي:

خ س م = م × خ = ٠,٠٠٠٥ × ١٠,٠٠٠,٠٠٠ = ٥٠٠٠ ريال

وكمثال آخر فإن احتمال حدوث خطأ لا يتم اكتشافه في إدخال حــرف واحد عن طريق لوحة المفاتيح يمكن أن يكون بمعدل مرة واحدة في الدقيقــة على مستوى المؤسسة، أي ٣٠٠ مرة في يوم العمل، أي ١٥٠٠ مــرة فــي الأسبوع، أي أن (م = ٧٨,٠٠٠) وهو عدد مرات حدوث الخطأ أو الأخطاء سنويًا. ولنفرض أن هذا الخطأ أو الأخطاء يكلف المؤسسة عند حدوثه نصف ريال أي أن (خ = ٠,٥) فبذلك تكون الخسارة السنوية المتوقعة كما يلي:

خ س م = م × خ = ٧٨,٠٠٠ × ٠,٥ = ٣٩,٠٠٠ ريال سنويًا

وهكذا يمكن تعميم هذا الأسلوب على جميع أصول المؤسسة المعرضة للتلف أو التأثر بالكوارث.

بالنسبة لمحاولات الانتهاك المتعمدة مثل: محاولة التعرف على كلمــة السر، أو محاولة اقتحام غرفة الحاسب، فإنه يلزم أن نقوم بتعديل المعادلــة السابقة (خ س م = م × خ) لتصبح:

خ س م = م × ن × خ

حيث ن = احتمال نجاح عملية الانتهاك، وبذلك ندخل عنصر احتمــال النجاح فإذا كان احتمال النجاح معدومًا (ن = صفر) فإن ذلك يجعل تقديــر الأخطار أو خ س م صفرًا، وفي هذه الحالة يمكن إهماله.

٥- تحليل الأنظمة الحرجة

(Mission Critical Systems)

٥-١- تحديد الأنظمة الحرجة

توجد في كل مؤسسة بعض نظم التطبيقات الحرجة أو الحساسة والتي يؤدي توقفها إلى نتائج غير مرغوب فيها، **ويعتبر التطبيق حرجًا إذا كان :**

١) تعتمد عليه المؤسسة في تلبية احتياجاتها.

٢) يتأثر به أداء الموظفين الأساسيين بشدة.

٣) مطلبًا أساسيًا لتنظيم العمل.

٤) يحافظ على الصورة العامة للمؤسسة.

٥) يمنح المؤسسة القدرة على المنافسة.

٦) يؤثر بشدة على الخدمة المقدمة لعملاء المؤسسة.

٧) يؤثر بشدة على الدخل المالي للمؤسسة.

٨) يترتب على توقفه آثار قانونية إما للعملاء أو للمؤسسة.

٩) لا يمكن إحلاله بنظام يدوي.

١٠) يتطلب معالجة أحجام ضخمة من البيانات.

١١) يتعامل مع البيانات بالأسلوب المباشر (Online) ولا يمكن أن يتم بأسلوب الدفعات (Batch) .

١٢) حرجًا بالنسبة لنظام آخر.

١٣) يتطلب تكلفة عالية لاستعادة النشاط.

أما النظم غير الحرجة بالنسبة للمؤسسة فلا تُعامل بنفس الاهتمام، **ويكون النظام غير حرج في الأحوال الآتية:**

١) إذا لم ينطبق عليه أي شرط من شروط النظم الحرجة.

٢) إذا كان من الممكن الاستغناء عنه لبضعة أسابيع.

٣) إذا وُجد له بديل (يدوي أو غير يدوي).

٥-٢- مثال تطبيقي لتحديد الأنظمة الحرجة

يبين الجدول (٦-٤) مثالاً تطبيقيًا لكيفية تحديد الأنظمة الحرجة من بين أنظمة المؤسسة.

شروط النظام الحرج	متابعة الخطة الخمسية	تلبية احتياجات العملاء	الرواتب	متابعة التدريب	الاتصالات الإدارية
١) تعتمد عليه المؤسسة لتلبية احتياجاتها.	نعم	نعم	لا	لا	لا
٢) يتأثر به أداء الموظفين الأساسيين بشدة.	لا	نعم	نعم	لا	لا
٣) يعتبر مطلباً أساسياً لتنظيم العمل.	نعم	نعم	لا	لا	لا
٤) يحافظ على الصورة العامة للمنظمة.	نعم	نعم	لا	لا	نعم
٥) يمنح المؤسسة القدرة على المنافسة.	نعم	نعم	لا	لا	نعم
٦) يؤثر بشدة على الخدمة المقدمة للعملاء.	لا	نعم	لا	لا	لا
٧) يؤثر بشدة على الدخل المالي.	لا	نعم	لا	لا	لا
٨) يترتب على توقفه آثار قانونية.	لا	نعم	نعم	لا	نعم
٩) لا يمكن إحلاله بنظام يدوي فعال.	لا	لا	لا	لا	لا
١٠) يقوم بمعالجة أحجام ضخمة من البيانات.	لا	نعم	نعم	لا	نعم
١١) يتعامل مع البيانات بنظام "الاتصال المباشر" (Online).	نعم	نعم	نعم	نعم	لا
١٢) يعتبر حرجا بالنسبة لأنظمة أخرى.	لا	نعم	نعم	لا	لا
١٣) يتطلب تكلفة عالية لاستعادة النشاط.	لا	نعم	نعم	لا	نعم
١٤) لا يوجد له بديل يدوي ولا يمكن الاستغناء عنه لعدة أسابيع.	لا	لا	لا	لا	لا
النتيجة	حرج	حرج	غير حرج	غير حرج	غير حرج

جدول رقم (٦-٤): مثال لتحديد الأنظمة الحرجة

تم التوصل إلى بيانات الجدول السابق من خلال المقابلات مع إدارة أمن المعلومات وإدارة الدعم الفني، وإدارة خدمات المستفيدين بالإضافة إلى بعض الإدارات المستفيدة وأمكن بذلك تحديد النظم الحرجة بالمؤسسة على النحو الذي يبينه الجدول (٦-٥):

اسم النظام	سبب الأولوية	هل هو حرج؟	درجة الأهمية	ملاحظات
نظام متابعة الخطة الخمسية	النظام يتابع سير العمل ويتأثر تحقيق المؤسسة لأهدافها بغيابه.	نعم	٩٠%	تنطبق على النظام معظم الشروط اللازمة لاعتباره نظامًا حرجًا.
نظام تلبية احتياجات العملاء	أهم أنشطة المؤسسة على الإطلاق، ويتوقف على نجاحه تحقيق المؤسسة لمعظم أهدافها.	نعم	١٠٠%	تنطبق على النظام معظم الشروط اللازمة لاعتباره نظامًا حرجًا، كما أنه يعتبر حرجًا بالنسبة لأنظمة أخرى.
نظام الرواتب	يمكن تنفيذه يدويًا.	لا	٣٠%	لا تنطبق عليه الكثير من شروط الأنظمة الحرجة.
نظام متابعة التدريب	يمكن تنفيذه يدويًا، كما يمكن الاستغناء عنه لفترة.	لا	٣٠%	لا تنطبق عليه الكثير من شروط الأنظمة الحرجة.
نظام متابعة الاتصالات الإدارية	النظام هام للحفاظ على صورة المؤسسة ولكن يمكن إحلال نظام يدوي مكانه لفترة.	لا	٦٠%	برغم انطباق بعض شروط الأنظمة الحرجة عليه فإنه ليس أكثر النظم حرجًا في المؤسسة.

جدول رقم (٦-٥): النظم الحرجة المختارة للمؤسسة

وبذلك تم اختيار نظامي متابعة الخطة الخمسية وتلبية احتياجات العملاء باعتبارهما الأنظمة الحرجة الرئيسية بالمؤسسة.

٦- إجراءات حماية الأصول

الآن وبعد تنفيذ الخطوات السابقة أصبحنا نعلم نوعية المخاطر التي تهدد المؤسسة ومقدار تعرضها لهذه المخاطر في غياب الضوابط المختلفة، ويجب عندئذ ترتيب مناطق التعرض بشكل تنازلي وفقًا لتأثيرها على العمل الأساسي للمؤسسة. ثم عن طريق فحص هذه المناطق بهذا الترتيب التنازلي يمكننا تحديد أفضل السبل للتعامل مع كل خطر لتحقيق درجة معينة من درجات التعامل مع الأخطار وتقليل أثرها، علمًا بأن الإجراءات المضادة التي تتخذ لتوقي خطر معين قد تؤدي في الوقت نفسه إلى تقليل أثر خطر آخر، فمثلاً إذا أنشأنا ضوابط استخدام جيدة لقاعدة البيانات فإن ذلك ــ إلى جانب تأمين سرية البيانات ــ سيؤدي أيضًا إلى تقليل فرص التزوير.

وفيما يلي الدرجات المختلفة للتعامل مع الأخطار وتقليل أثرها:

٦-١- منع الخطر بالكامل

وهو أكثر هذه الدرجات فاعلية لأنه يهدف إلى استئصال الخطر من جذوره، وفي بعض الأحيان قد يتعذر تحقيق هذا الهدف بشكل عملي أو قد يكلف الكثير من المال أو الأفراد لتطبيق الإجراءات المطلوبة وفرض تنفيذها باستمرار. فمثلاً لمنع إساءة استخدام أسلوب الاتصال عن بعد (أي الدخول إلى نظام الحاسب عن طريق الهاتف من خارج المؤسسة) قد تلجأ المؤسسة إلى منع الشركة الموردة للحاسب خلال عمليات الصيانة من استخدام أسلوب (التشخيص عن بعد Remote Diagnostics)، وقد تلجأ المؤسسة إلى منع مبرمجي الصيانة من استرجاع بعض البيانات التجارية أو البرامج عن طريق الحاسبات الشخصية من منازلهم، وفي الحالتين ترتفع تكاليف الصيانة (سواء صيانة الأجهزة أو البرامج) وتزداد مدة التأخير في إنجازها ربما إلى حد غير مقبول.

٦-٢- تقليل الخطر

وهو ما نلجأ إليه إما لتقليل معدل حدوث الخطر أو لتحديد أثر التلف أو الخسارة المالية في حالة حدوثه، ففي المثال السابق عن الاتصال عن بعد قد تفضل المؤسسة السماح بالاتصال عن بعد فقط عن طريق المشغلين الذين يقومون بأنفسهم بطلب مهندس الصيانة ثم توصيله هاتفيًا بوحدة التشخيص مع تقييد هذا الاتصال ليكون مقصورًا على الوحدة المعطلة فقط مثل القرص الممغنط، أو البرامج المطلوب صيانتها فقط بعد فصلها عن باقي النظام. وبعد الانتهاء من عملية الصيانة مباشرة يتم فصل الخط ومنع الاتصال.

٦-٣- اكتشاف الخطر والتحرك لمواجهته

ربما كان هذا الهدف أضعف من سابقيه حيث إن الضرر يكون قد وقع بالفعل، ولكن من ناحية أخرى فربما ينتج عن التحديد المبكر أن تتمكن المؤسسة من احتواء الضرر الواقع أو الوقت المهدر ، وإلا فإن الضرر ربما يكون أكثر شدة أو تتصاعد الخسارة بلا توقف، وغني عن البيان أن التحديد المبكر لا يكفي وحده وإنما لابد أن تتبعه إجراءات التصحيح الضرورية للتعامل مع حالات الخطر المختلفة وفقًا لدرجة خطورتها ومدى استعجالها. فإذا أخذنا التقرير الشهري لمحاولات الدخول غير المشروعة للنظام على سبيل المثال، ليس من المحتمل أن يكشف هذا التقرير مقتحمًا من خلال محاولاته المستمرة لاقتحام النظام أثناء إجرائه لهذه المحاولات، ولكن المفروض أن يخبرنا نظام الكشف أن هناك محاولات "جرت" وما هو نوع هذه المحاولات وأي جزء من النظام كان مستهدفًا بها، وفي هذه الحالة لابد من وجود إجراءات معدة سلفًا تتخذ لمعالجة الأمر.

٦-٤- استعادة النشاط

برغم الجهود العديدة وجميع الاحتياطات التي تتخذ تبقى هناك دائمًا فرصة ولو ضئيلة لحدوث المخاطر أو وقوع الحوادث، وهنا يأتي دور خطة الطوارئ في المؤسسة.

عند تحديد الاحتياجات الأمنية لنظام جديد من الضروري أن تُؤخذ الإجراءات الاحتياطية وإجراءات استعادة النشاط في الاعتبار في المراحل المبكرة من التخطيط (مرحلة التصميم مثلاً)، وقد يؤثر هذا كثيرًا على أسلوب تصميم النظام بما يجعله أكثر أمنًا، فهذا هو الوقت المناسب لإدخال هذه الاحتياطات بأقل تكلفة وأقل مجهود وأفضل نتيجة.

٧- البدائل الاحتياطية

٧-١- مفهوم البديل الاحتياطي

تلجأ بعض المؤسسات إلى تأمين بديل كامل لضمان استمرارية العمل، والبديل الكامل هنا هو نظام حاسب آلي كامل (جهاز الحاسب وأجهزة التخزين والبرامج و...)، وهذا البديل قد يكون ملكًا للمؤسسة وهنا تصبح التكلفة عالية فهي تكاد تماثل تكلفة النظام الأصلي، وقد يكون هذا البديل موجودًا لدى جهة أخرى ويمكن استخدامه وفقًا لاتفاق مبرم مع تلك الجهة، وهذا يخفض التكلفة كثيرًا ولكن درجة استعداده الفوري للعمل تكون محدودة بمعنى أن الوقت الذي تحتاجه المؤسسة لإعداد الحاسب البديل ليكون جاهزًا للعمل هو أكثر بكثير من الحالة الأولى التي تمتلك فيها المؤسسة حاسبًا كاملاً يقبع في انتظار وقوع الكارثة!! وكثيرًا ما تتفق مؤسستان على أن يكون الحاسب الآلي الخاص بكل منهما بديلاً للمؤسسة الأخرى في حالة الكوارث وهذا يخفض التكلفة إلى حد بعيد.

٧-٢- ما هي البدائل المتاحة ؟

١) ألا نفعل شيئًا

- هو أرخص الحلول ولكنه يعتمد على طبيعة العمل.
- هو حل قد تكون آثاره خطيرة، وعادة لا يغطي التأمين هذه الآثار بالكامل.
- لا يمكن التعويض عن فقد العملاء أو فقد مصداقية المؤسسة.
- سوف يستفيد المنافسون من الظرف السيئ الذي حاق بالمؤسسة.

٢) المركز البديل غير الفوري (Cold Site)

هذا المركز البديل قد يكون مشتركًا مع مؤسسة أخرى أو خاصًا بالمؤسسة نفسها، وهو لا يكون جاهزًا للتشغيل على الفور، ولكنه يحتاج إلى تجهيز وإلى فترة زمنية ليصبح جاهزًا، كما يتطلب الأمر شراء بعض المعدات الإضافية وتركيبها.

- هذا الحل رخيص نسبيًا.
- قد لا يحتوي على جميع التسهيلات التي كانت موجودة في المركز الأصلي.
- ليست هناك فرصة لإجراء اختبارات مسبقة للتأكد من فعالية هذا البديل.
- التأخير الناتج عن توفير المعدات المطلوبة غير محكوم.

٣) المركز البديل نصف الفوري (Warm Site)

- التشارك مع جهة أخرى في استخدام الحاسب.
- توفر تسهيلات كاملة.

- صعوبة إجراء الاختبارات ولكن إجراءها ليس مستحيلاً.
- إذا كانت الأقراص الممغنطة ثابتة فإن ذلك يتطلب استمرار الاحتفاظ بنسخ احتياطية متجددة دائمًا للأقراص الأصلية.
- ليست هناك ضمانات كاملة للتشغيل، فقد تحتاج المؤسسة الأخرى للمركز البديل في نفس الوقت ولا يمكنها الاستغناء عنه ، أو ربما قد نفاجأ بتغييرات غير متوقعة لم يتم الاستعداد لها، أو قد يحدث تضارب بين احتياجات المؤسسات المتشاركة.

٤) المركز البديل الفوري (Hot Site)

- هذا هو البديل الوحيد المضمون بالكامل.
- مركز آمن مجهز بالكامل بجميع المعدات.
- جهاز حاسب آلي غير مستخدم ومخصص بالكامل لأغراض استعادة النشاط.
- الجهاز ونظام التشغيل وإجراءات استعادة النشاط مختبرة بالكامل ويجري اختبارها من آن لآخر.
- إجراءات هذا الأسلوب منظمة جدًا إذ يعتمد على إجراءات محددة ومعروفة ومعلنة ومختبرة يتم اتباعها عند الحاجة.

٧-٣- متطلبات المركز البديل الفوري

١) توفر موقع بديل داخل مبنى المؤسسة أو خارجه.

٢) نظم بديلة منفصلة ولكنها متضمنة بالكامل في جهاز الحاسب الخاص بالمؤسسة.

٣) أن يقوم مختصو الحاسب بالمؤسسة بتقديم نفس الخدمة المعتادة بأنفسهم لعملاء المؤسسة.

٤) أن يكون هناك المزيد من التسهيلات الإضافية والمزيد من الخدمات الإضافية ومن الدعم الإضافي أكثر مما يحتاجه المركز.

٥) أن تلتزم الجهة التي تقدم المركز البديل الفوري بتقديم الخدمة فور احتياجها وأن تتعاون طوال الوقت بتنفيذ ما يلزم من تعديلات أو إضافات حتى يصبح المركز البديل أقرب ما يكون إلى المركز الأصلي.

٧-٤- أسباب عدم نجاح المركز البديل

١) قد يكون موقع المركز البديل قريبًا جدًا من المركز الأصلي.

٢) قد تصاب وسائط التخزين الاحتياطي أو تتأثر بنفس الكارثة.

٣) المركز البديل معرض أيضًا للأخطار.

٤) قد يكون من الصعب فرض اتباع القواعد والنظم إذ أن معظم المؤسسات تقوم بتقييم موظفيها على أساس مقدرتهم على تقديم الخدمة وليس على أساس كفاءتهم في استعادة النشاط بعد الكارثة، لذلك قلما تُجرى الاختبارات اللازمة للمركز البديل.

٥) الموظفون الذين يديرون المركز البديل قد لا يكونون من الخبراء في استعادة النشاط بعد الكارثة، وربما لا تكون لديهم أي خبرة في هذا المجال.

٦) أحيانًا يكون من الصعب تبرير اقتناء جهاز ثانٍ بالكامل لمجرد استعادة النشاط بعد الكارثة، ولذلك يُشترى هذا الجهاز لحساب التطوير وينتهي الأمر بأن يصبح جهازًا ثانيًا من أجهزة المركز.

٧) ربما كان من الصعب تبرير الاحتفاظ بجهاز ثانٍ بالمؤسسة بنفس مكونات (H/W configuration) الجهاز الأول، فيتم تقليص إمكانات الجهاز الاحتياطي.

٧-٥- تَشارُك المؤسسات في البديل الاحتياطي

تلجأ بعض المؤسسات التي لديها مكونات متشابهة وأنظمة تشغيل متشابهة في الحاسب الآلي الخاص بها إلى التشارك في بديل احتياطي تستخدمه المؤسسة التي يتعطل الحاسب فيها عن العمل لفترة محسوسة تحتاج خلالها لتشغيل أنظمتها باستخدام نظام بديل، ويعتبر هذا الحل أرخص بشكل كبير من الانفراد ببديل احتياطي تكون تكلفته عالية.

ويبين الجدول (٦-٦) احتمالات المخاطرة التي تتعرض لها كل مؤسسة في حالة وجود جهاز احتياطي بديل (أو أكثر) تتشارك فيه عدة مؤسسات:

عدد الأجهزة الاحتياطية	عدد المؤسسات المتشاركة	احتمال أن تحتاج إليه مؤسسة فتجده مشغولاً (*)
جهاز واحد	٢٥	٢٥٠ في كل عشرة آلاف (٠,٢٥ %)
جهازان	٢٥	٢٥ في كل مليون (٠,٠٠٢٥%)

(*) بفرض أن احتمال حدوث الكارثة هو ١%

جدول (٦-٦) احتمالات المخاطرة في حالة وجود جهاز احتياطي بديل تتشارك فيه عدة مؤسسات

يتبين من هذا الجدول أنه إذا كان احتمال حدوث الكارثة هو ١%، ففي حالة اشتراك خمس وعشرون مؤسسة في هذا الجهاز فإن احتمال أن تحتاج إليه مؤسسة فتجده مشغولاً هو:

الاحتمال = ٠,٠١ × ٠,٠١ × ٢٥ = ٠,٢٥%

وإذا تشارك نفس العدد من المؤسسات (٢٥ مؤسسة) في جهازين فإن احتمال أن تحتاج إليه مؤسسة فتجده مشغولاً هو:

الاحتمال = ٠,٠١ × ٠,٠١ × ٠,٠١ × ٢٥ = ٠,٠٠٢٥%

الفصل السابع

خطة الطوارئ المعلوماتية

موضوعات الفصل:

(١) أهداف خطة الطوارئ.

(٢) عوامل نجاح خطة الطوارئ.

(٣) محتويات خطة الطوارئ.



نتحدث في هذا الفصل عن خطة الطوارئ المعلوماتية، والتي لابد من وجودها لدى كل مركز حاسب آلي تحسبًا للطوارئ. فنستهل الفصل بشرح المقصود بخطة الطوارئ وبتحديد أهداف هذه الخطة، كما نبين التكلفة التراكمية لعملية استعادة النشاط العادي في المؤسسة، وكيفية الوصول إلى أدنى تكلفة، كما نتحدث عن عوامل نجاح أو فشل خطة الطوارئ، ونقدم الوصايا العشر للإدارة العليا في هذا الصدد، ثم نختتم الفصل بما يجب أن تحتوي عليه خطة الطوارئ.

١- أهداف خطة الطوارئ

أوضحنا في الفصل الخامس كيف أن المبادئ الأساسية لنجاح نشاط مواجهة الكوارث يمكن تلخيصها في:

١) الحصول على التزام الإدارة العليا.

٢) توفير الميزانية اللازمة.

٣) إيجاد موقع تشغيل بديل.

٤) إجراء اختبارات استعادة النشاط باستمرار.

٥) إعداد خطة طوارئ ناجحة.

وسنركز في هذا الفصل على المبدأ الأخير وهو **إعداد خطة طوارئ ناجحة.**

١-١- خطة الطوارئ

خطة الطوارئ (Contingency plan) هي خطة مكتوبة ومعتمدة

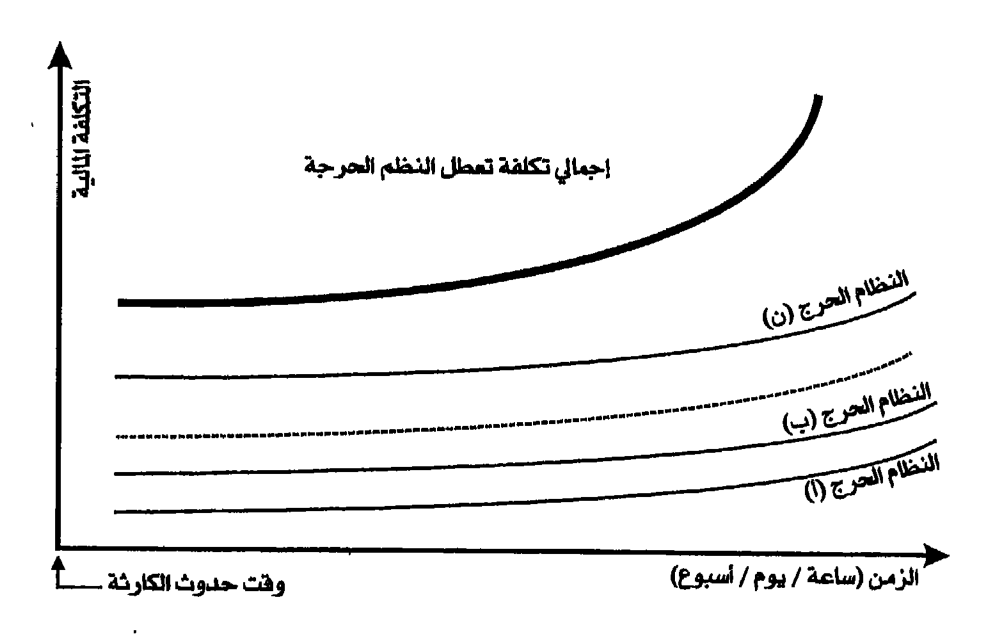
ومعدة للتنفيذ ويتم اختبارها باستمرار، وهي تحدد كافة الإجراءات الواجب اتخاذها لتحسين درجة مقاومة المؤسسة للأخطار وتقليل الخسائر الناتجة عن الكارثة إلى الحد الأدنى، وفي هذه الخطة نتعامل مع أحداث ممكنة الحدوث ولكن احتمال حدوثها ليس كبيرًا. وتعتبر خطة مواجهة الطوارئ هي نهاية المطاف في نشاط مواجهة الكوارث في أي مؤسسة والهدف منها **تمكين المؤسسة من استعادة نشاطها في أقل وقت وبأقل تكلفة.**

ذكرنا أن الهدف الأساسي لخطة الطوارئ هو استعادة نشاط المؤسسة **في أقصر وقت وبأقل تكلفة** وبالطبع فإن هذين المطلبين متعارضان، فإذا أردنا استعادة فورية فهذا سيتطلب تكلفة ضخمة كما بينا من قبل، ولذلك لابد من الحساب الدقيق لهذين العاملين (سرعة استعادة النشاط والتكلفة المطلوبة) والعلاقة بينهما حتى يمكن التوصل إلى **حل أفضل** يوازن بينهما.

١-٢- التكلفة التراكمية لتعطل النظم الحرجة

يمثل الشكل (٧-١) **التكلفة التراكمية لتعطل النظم الحرجة** في المؤسسة، فالمنحنى المبين يمثل العلاقة بين الآثار المتراكمة للعطل مع مرور الوقت بعد حدوث الكارثة، ويلاحظ أن التكلفة التي تتحملها المؤسسة هي دالة لنوع العطل الذي أصاب الأصول. وتختلف وحدات الوقت التي يمكن استخدامها من دقائق أو ساعات أو أيام حسب حجم المؤسسة وجسامة العطل، ويمكننا من خلال هذا المنحنى تحديد مدة التعطل المسموح بها قبل أن تستفحل مخاطر انهيار المؤسسة إذا ما استمر العطل إلى حدود غير مقبولة. ويراعى أن يُرسم هذا المنحنى للنظم الحرجة فقط دون غيرها وبافتراض أسوأ الحالات (كأن يحدث في أسوأ وقت وكأن يؤدي إلى فقدان كامل للنظام)، وميل المنحنى للأعلى هنا هو مؤشر لدرجة اعتماد المؤسسة على هذا النظام، فكلما زاد هذا الاعتماد زاد ميل المنحنى، كما أن وحدات

الزمن ترتبط هي الأخرى بدرجة هذا الاعتماد فكلما تضاءل الاعتماد كبرت هذه الوحدات.

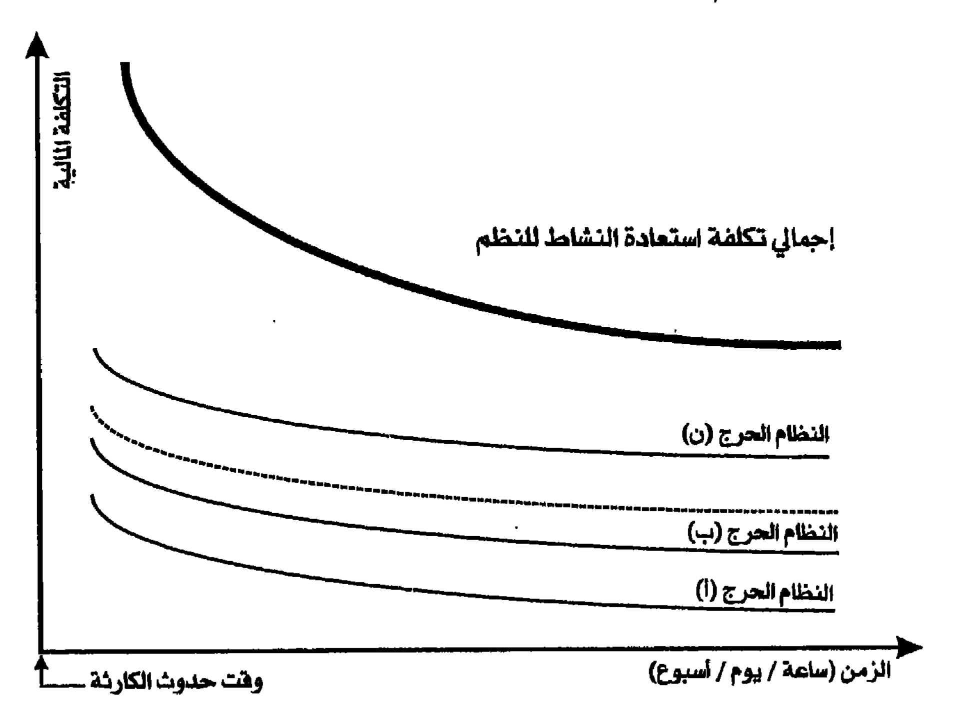


الشكل (٧-١) التكلفة التراكمية لتعطل النظم الحرجة

١-٣- التكلفة التراكمية لاستعادة النشاط

أما الشكل (٧-٢) فيمثل التكلفة التراكمية لاستعادة النشاط فالمنحنى المبين يمثل العلاقة بين تكلفة استعادة النشاط بعد الكارثة والوقت اللازم لذلك، وبشكل عام فهذه العلاقة عكسية كما ذكرنا، وهنا أيضًا يعتبر ميل المنحنى مؤشرًا لدرجة اعتماد المنشأة على النظام الحرج، وعند حساب التكلفة تؤخذ في الاعتبار قيمة التكاليف المرتبطة بجميع التدابير التي تم اختيارها لمواجهة الأعطال (مثل تكرار الأصول داخل الموقع، إيجاد موقع

بديل، توفير وسائط تخزين احتياطيـــة، ...) أي أن هـــذا المنحنـــى يمثـــل باختصار التكلفة التقديرية لعملية استعادة النشاط باستخدام البدائـــل المختلفـــة (الفوري، نصف الفوري، أو غير الفـــوري) ويراعـــى أن تســـتخدم نفـــس الوحدات عند رسم كل من المنحنيين.

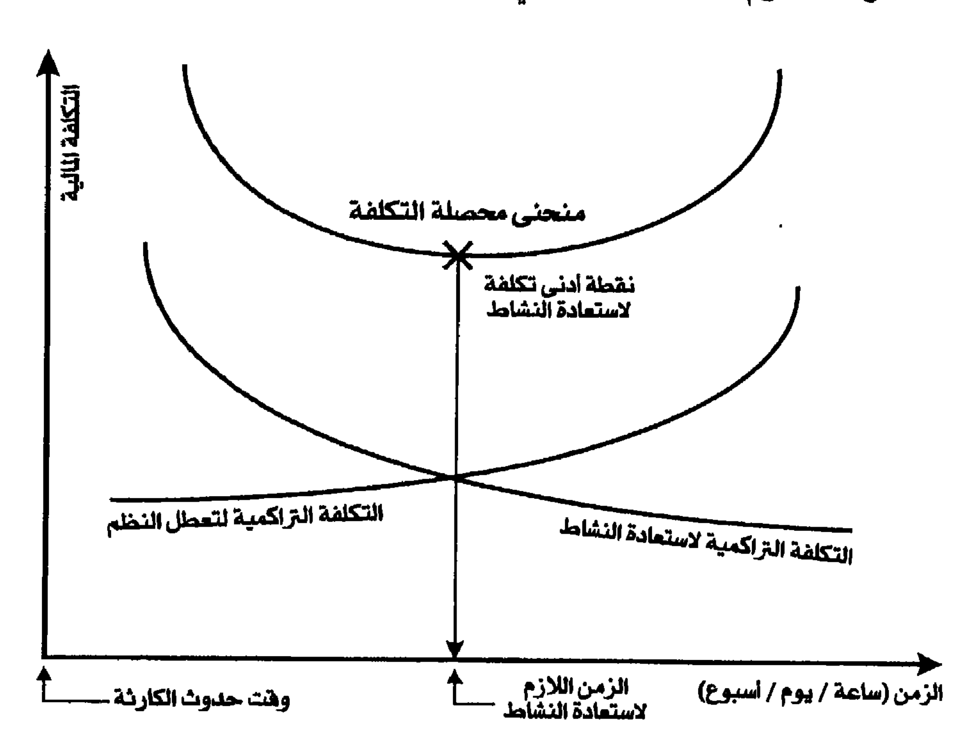


شكل (٧-٢) التكلفة التراكمية لاستعادة النشاط

١-٤- أدنى تكلفة لاستعادة النشاط

ولابد لنا الآن من الموازنة بين كلا المنحنيين، ويمثل الشـــكل (٧-٣) محصلة المنحنيين السابقين إذ يمثل منحنى محصلة التكلفة مجموع منحنـــى

تكلفة الأعطال ومنحنى تكلفة استعادة النشاط، وتمثل أدنى نقطة على منحنى محصلة التكلفة الحد الأدنى لإجمالي تكلفة الأعطال وهي تمثل في الوقت نفسه الوقت اللازم لاستعادة النشاط في حدود هذه التكلفة.



شكل (٧-٣) أدنى تكلفة لاستعادة النشاط

١-٥- العوامل التي تساهم في ارتفاع التكلفة

١) شدة اعتماد المؤسسة على النظام (شدة ميل المنحنى).

٢) زيادة عدد النظم الحرجة في المؤسسة.

٣) قصر الوقت المسموح به لتحمل العطل.
٤) ارتفاع تكلفة البدائل التي تم اختيارها.
٥) الافتقار إلى النظرة الشاملة عند اختيار البديل المناسب حيث تم اختيار بديل لكل نظام.

١-٦- العوامل التي تساهم في زيادة وقت استعادة النشاط

١) طول الفترة اللازمة لإعداد الموقع البديل إذا كان مستوى إعداده غير مناسب (غير فوري / نصف فوري).
٢) طول الفترة اللازمة لتطبيق إجراءات المساندة واستعادة البيانات.
٣) محاولة ضغط النفقات باختيار وسائل احتياطية بطيئة مثلاً.

٢- عوامل نجاح خطة الطوارئ

هناك عدة عوامل يجب أخذها في الاعتبار لضمان نجاح خطة الطوارئ والعامل الأول والأهم هو:

٢-١- ضمان دعم الإدارة العليا للخطة

دعم الإدارة العليا لخطة الطوارئ يلعب دوراً كبيرًا في ضمان نجاح هذه الخطة، وللحصول على ذلك يجب :

١) عرض الخطة على الإدارة العليا مع تحليل كامل للأخطار.
٢) مشاركة الإدارة في مفهومها عن أيّ الوظائف (أو التطبيقات)

تعتبر حرجة (حساسة) بالنسبة للعمل الرئيسي للمؤسسة.

٣) التبرير المالي الجيد (عن طريق تحليل الخسائر السابقة ومقارنة تكلفة التعطل مع تكلفة استعادة النشاط).

٢-٢- باقي العوامل التي يجب أخذها في الاعتبار

١) محاولة تقليل خطر حدوث الكارثة إلى أدنى حد ممكن.

٢) زيارة المواقع البديلة وتفقدها باستمرار.

٣) توعية الموظفين والعاملين بأهمية هذا النشاط (بالمقالات والنشرات والندوات والاجتماعات الدورية).

٤) المراقبة المستمرة للخطة وإجراء الاختبارات اللازمة عليها للتأكد من نجاحها عند الحاجة إليها.

٥) تحديد الموارد اللازمة للحفاظ على استمرارية التشغيل بدقة والتأكد من أن الحصول على هذه الموارد ممكن وميسور وفي وقت مناسب ومتفق عليه.

٦) نشر خطة استعادة النشاط على جميع المستويات وتلقي آراء الموظفين بشأنها وأخذ هذه الآراء في الاعتبار عند المراجعة الدورية للخطة.

٧) تدريب الأفراد على تنفيذ الخطة واختبارها.

٨) المرونة في إعداد الخطة والواقعية في تقدير الأخطار وتحديد الزمن اللازم لاستعادة النشاط واقتناع المستفيدين به.

٩) محاولة تقليص الصدمة التي تتلو الكارثة إلى أدنى حد مما يسمح باستعادة النشاط بسرعة أكبر.

١٠) أن تكون الخطة مناسبة **لاحتياجات وطبيعة العمل الأساسي** للمؤسسة.

١١) أن تكون الخطة جاهزة ومعدة للتنفيذ قبل حدوث الكارثة.

١٢) أن يكون الهدف الرئيسي للخطة دائمًا هو **العمل الرئيسي** للمؤسسة وليس مجرد استعادة نشاط الحاسب الآلي.

٢-٣- عشر وصايا للإدارة العليا

هذه الوصايا العشر موجهة للإدارة العليا لضمان نجاح خطة الطوارئ:

١) الحاجة إلى تقييم الأخطار المحدقة بالعمل نتيجة تعطل الحاسب، من أجل تحديد المناطق الحرجة ومن أجل تأكيد كم تطول المدة التي يمكن أن يتحملها كل قسم بدون خدمات الحاسب الآلي. وعندئذ فقط يمكن للإدارة أن تحدد حجم وطبيعة خطة مواجهة الطوارئ المطلوبة. هذه المهمة يجب أن يقوم بها الرئيس الأعلى للمؤسسة ولا يجب أن تترك لمتخصصي الحاسب الآلي الذين يجب أن تتركز مهامهم على تطبيق واختبار الخطة التي يتم الاتفاق عليها.

٢) تحتاج خطة الطوارئ إلى أن تتم مراجعتها بصفة مستمرة لأن هناك تغيرات تحدث باستمرار في طبيعة العمل وطبيعة النظم الحرجة بل ونوعية الأخطار نفسها. هذه التغيرات يجب مواكبتها ومراجعة الخطة على ضوئها حتى تصبح الخطة حديثة باستمرار.

٣) تحتاج خطة الطوارئ إلى أن يتم اختبارها بصفة مستمرة وأن يشارك في اختبارها المستفيدون من الإدارات الأخرى الذين يعملون في مجال العمل الرئيسي للمؤسسة إلى جانب متخصصي الحاسب الآلي.

٤) يجب على الإدارة العليا وضع الآلية اللازمة للتأكد من أن مراجعة الخطة وكذلك اختبارها يتم أداؤهما بالفعل وعلى فترات مناسبة.

٥) يجب على الإدارة العليا عند إعداد الخطة الإنصات إلى **نصيحة من خارج المؤسسة** ، إذ إن شخصًا من خارج الصورة يكون قادرا على اقتراح أشياء قد تغيب عن الموظفين من داخل المؤسسة.

٦) يجب أن يتضمن التخطيط الإجراءات التي تكفل إزالة أو على الأقل تقليل أكبر مناطق الخطر، فإذا كان نظام الرواتب مثلاً هو أكبر نظام حرج للمؤسسة ولا يمكن تحمل توقفه، فمن الممكن أن يسند القيام بهذا النظام بالكامل إلى مؤسسة حاسب متخصصة في نظم الرواتب إذا كان لديها مستوًى عال من الإجراءات الاحتياطية أو تملك البديل الفوري الجاهز الذي لا يمكن توفيره داخل المؤسسة.

٧) بمجرد حدوث الكارثة يجب أن تضمن الإدارة العليا أن يتم تصعيد المشكلات في السلم الإداري بأسرع ما يمكن، لأنه في جميع المستويات الإدارية يوجد نوع من التردد الطبيعي في الاعتراف بأن الموقف لا يمكن التعامل معه في هذا المستوى ويجب تصعيده إلى المستوى الإداري الأعلى، والشيء نفسه ينطبق كذلك على مهندسي الصيانة من الشركات الموردة الذين يترددون في تصعيد المشكلة للمستويات الأعلى في الشركة الموردة فور حدوثها.

٨) لا يجب التقليل من شأن المشكلات التي تنشأ خلال عملية معالجة الكوارث وخاصة عندما يتأثر أكثر من موقع بهذه الكارثة.

٩) يجب أن تفترض الإدارة العليا الأسوأ دائمًا وألا تصدق التوقعات المفرطة في التفاؤل التي يقدمها متخصصو الحاسب الآلي.

١٠) فوق كل ما سبق، يجب في حالة حدوث كارثة شاملة، لا قدَّر الله، أن تتوخى الإدارة العليا الحسم في اتخاذ القرار وتجنب الفزع والاضطراب.

٢-٤- الاهتمام الحالي بخطة الطوارئ

من واقع خبرتي في التحاور مع العديد من مسئولي الوزارات والشركات المختلفة في المملكة العربية السعودية خلال تدريسي لبرنامج "أمن الحاسبات" وتدريسي لحلقة "أمن المعلومات" في معهد الإدارة العامة، وكذلك في العديد من البلدان العربية خلال تدريسي لدورات عن جرائم الحاسب الآلي في "أكاديمية نايف للعلوم الأمنية" التي تقدم برامجها لمسئولي أمن المعلومات في الدول العربية الأعضاء في جامعة الدول العربية، ومن خلال محاضراتي في جمعية الحاسبات السعودية في نفس المجال، من خلال ذلك أستطيع أن أؤكد أن عدداً محدوداً من هذه الجهات (حوالي ٢٥%) لديها خطة طوارئ جاهزة، ولكن كم من هذه الخطط يعمل بالكفاءة المطلوبة ؟

كما تبين الإحصاءات أن ٩٠% من المؤسسات التي عانت من كوارث قضت على غرفة الحاسب الآلي فيها، ولم تكن لديها في ذلك الوقت خطة طوارئ جاهزة، قد **خرجت من المنافسة** في مجال نشاطها خلال ثمانية عشر شهرًا من وقوع الكارثة [Martin-1989].

٣- محتويات خطة الطوارئ

يجب أن يحتوي التقرير المقدم عن خطة الطوارئ بصفة عامة على الأقسام التالية:

١) **مقدمة تشمل ما تغطيه الخطة والتزام الإدارة العليا والجهات المشاركة في تنفيذ الخطة.**

٢) **أهداف الخطة وتشمل الأولويات وأهداف المؤسسة والنشاط الرئيسي لها والنظم الحرجة التي تؤثر على أداء المؤسسة.**

٣) **تحليل الأخطار.**

٤) **تحليل النظم الحرجة.**

٥) **إجراءات الطوارئ.**

٦) **مهام الفرق المختلفة المشاركة في الخطة مثل فرق الاتصالات وغيرها.**

٧) **أسلوب اختبار الخطة.**

٨) **أسلوب صيانة الخطة وأسلوب إدخال التعديلات عليها.**

٩) **أسلوب تدريب الموظفين على تنفيذ الخطة عند وقوع الكارثة.**

١٠) **أسلوب مراقبة الخطة ومراجعتها.**

١١) **ملاحق الخطة وتشمل قوائم المشاركين في تنفيذها وقوائم بالإمكانيات المتاحة ومكونات النظام البديل والميزانية المخصصة وقوائم بعملاء المؤسسة ومختلف البيانات الأساسية المطلوبة.**

ويعتبر أهم أقسام تقرير الخطة هو القسم الخاص بإجراءات الطــوارئ أي الإجراءات التي يتم تنفيذها بالترتيب عند وقوع الكارثة، وهـــو عصـــب الخطة كلها، ولذلك سنفرد له فصلاً خاصًا.

الفصل الثامن

تنفيذ خطة الطوارئ

موضوعات الفصل:

(١) إجراءات الطوارئ.

(٢) مهام المشاركين في فرق الطوارئ.

(٣) اختبار وصيانة ومراقبة خطة الطوارئ.

(٤) تدريب الموظفين على تنفيذ الخطة.



خصصنا هذا الفصل للحديث عن كيفية تنفيذ خطة الطوارئ، وهو بذلك يعتبر امتداداً للفصل السابق. ونبدأ الفصل بالحديث عن إجراءات الطوارئ بدءاً من إخلاء الموقع، ومروراً بإبلاغ الجهات المختصة والتقويم الأولي لآثار الكارثة وكيفية استعادة النشاط، وانتهاء بتشغيل الموقع البديل وإعادة الخدمة المعتادة للمستفيد. ثم ننتقل إلى الحديث عن فرق الطوارئ ومهام المشاركين في هذه الفرق، ثم كيفية اختبار خطة الطوارئ وصيانتها ومراقبة تنفيذها. ثم نختتم الفصل بالحديث عن أساليب تدريب الموظفين على تنفيذ الخطة.

١- إجراءات الطوارئ

١-١- إخلاء الموقع

بعد وقوع الكارثة مباشرة تبدأ أولى إجراءات الطوارئ، فإذا كانت الكارثة من النوع الذي يتطلب إخلاء الموقع فيجب أن تكون الخطوة الأولى لفريق الطوارئ هي تنفيذ عملية الإخلاء. ويتوقف حجم الإخلاء على حجم الكارثة نفسها؛ فقد يكون إخلاء عامًا لجميع العاملين في المؤسسة بما فيهم فريق الطوارئ أو يمكن استثناء فريق الطوارئ من الإخلاء وفي هذه الحالة على هذا الفريق أن يبدأ تنفيذ إجراءات الطوارئ الأساسية مثل تشغيل أجهزة مكافحة الحريق وأجهزة الخدمات الأساسية البديلة كالكهرباء والماء، ونقل الأصول الحساسة إلى مكان آمن وتأمين الأصول التي لا يمكن نقلها. وقد يكون الإخلاء غير فوري عندما لا تكون الكارثة مفاجأة فيتولى فريق الطوارئ إطلاق أجهزة الإنذار وإيقاف العمل في مركز الحاسب بسرعة ولكن بطريقة نظامية (Normal shutdown) وتكون لدى الفريق الفرصة لنقل الأشياء ذات القيمة وبعض وسائط المعلومات إلى أماكن آمنة.

١-٢- إبلاغ الجهات المختصة

يتم إبلاغ الجهات التي يجب أن تحاط علمًا بالكارثة إما للتدخل أو للتوقف عن العمل وهذه الجهات هي:

١) رئيس مركز الحاسب (أو من يمثله إذا وقعت الكارثة في إحدى نوبات العمل).

٢) الجهات الخارجية المعاونة في التصدي للكارثة كإدارة الحريق أو الدفاع المدني.

٣) مدير الإدارة المسئولة عن المقر لتقديم العون أو الإمداد بالعمالة المعاونة أو قطع الكهرباء أو تسهيل دخول رجال الإنقاذ أو غيرهم، وغير ذلك.

٤) مسئول أمن المعلومات وهو بالضرورة عضو في فريق الطوارئ.

٥) باقي أفراد فريق الطوارئ، والتأكد من تجمعهم وأن هناك بدلاء للغائبين منهم وأن كلاً منهم بدأ القيام بواجبه.

٦) مديرو الإدارات المستفيدة من المهددين بقطع الخدمة.

٧) المسئولون في الموقع البديل أو الجهة المسئولة عن تقديم الخدمة البديلة.

٨) شركات التأمين إذا كانت العقود تنص على ذلك.

ويجب عند تنفيذ عملية الإبلاغ الاتصال بهذه الجهات بالترتيب المذكور وإن كان يفضل الاتصال بهم على التوازي لتوفير الوقت، ووفقًا لحجم وطبيعة الكارثة قد يتم استثناء بعض هذه الجهات إذا لم توجد ضرورة لإخطارها.

كما يجب أن تتضمن ملاحق خطة الطوارئ ملحقًا خاصًا بأسماء الجهات المطلوب الاتصال بها عند وقوع الكارثة واسم الشخص المسئول فيها ورقم الهاتف ورقم الفاكس والعنوان مع وجود أسماء بديلة وأرقام بديلة باستمرار، ويمكن إعداد نسخة من هذه القائمة وتعليقها في مكان ظاهر في المؤسسة.

١-٣- التقويم الأولي لآثار الكارثة

يتم في هذه الخطوة تقويم أولي شامل لآثار الكارثة بالفحص السريع للأصول المختلفة للمؤسسة من أجهزة وبرمجيات وأفراد ومعلومات وغير ذلك بهدف تحديد الخسائر والأصول التي تعطلت تمامًا عن العمل والأصول التي يمكن إعادتها للعمل بسرعة وموقف النظم الحرجة ومدى الضرر الذي حاق بها. كما يتم في هذه الخطوة أيضًا تقدير الوقت المتوقع لاستعادة النشاط بالنسبة لكافة الأجهزة الحرجة والنظم الحرجة كذلك. ومطلوب من الفريق في هذه المرحلة أن يحدد مدى الحاجة إلى الموقع البديل أو الاكتفاء بإصلاح ما تلف في الموقع الأصلي.

١-٤- استعادة النشاط

يؤدي تقويم آثار الكارثة، الذي تم في الخطوة السابقة، إلى اختيار الأسلوب الذي سيتم به استعادة النشاط، فذلك إما أن يكون في نفس الموقع

وهنا يتم إخطار المستفيدين بالمدة التي سيستغرقها ذلك، أو سيتم تشغيل الموقع البديل وفي هذه الحالة يجب إخطار المسئولين عن ذلك الموقع بموعد الانتقال إلى هناك وإخطار المستفيدين بموعد استعادة النشاط، وفي بعض الأحيان قد يكون القرار هو نقل جزء من العمل فقط إلى الموقع البديل والإبقاء على الجزء الآخر في الموقع الأصلي. وتختلف إجراءات استعادة النشاط باختلاف الأصول كما يلي:

١-٤-١- الأجهزة

يتم استعادة النشاط عن طريق تشغيل الموقع البديل إذا كان فوريًا (Hot) أو إعداده للتشغيل إذا لم يكن كذلك، أي إذا كان غير فوري (Cold) أو نصف فوري (Warm). وبإتمام نشاط تقويم الخسائر ربما أمكن نقل بعض الأجهزة من الموقع الأصلي المتضرر بالكارثة إلى الموقع البديل، ويجب أن يكون واضحًا في خطة الإجراءات كل ما يلزم لتجهيز الموقع البديل وإعداده للعمل.

١-٤-٢- البيانات

بافتراض أن الكارثة قد قضت على جميع الملفات وقواعد البيانات يجب اللجوء إلى النسخ الاحتياطية المحفوظة في موقع بعيد عن الموقع المتضرر، ويجب أن تحدد إجراءات الطوارئ كيفية نقل وسائط البيانات الاحتياطية إلى الموقع وكيفية استعادة البيانات والبرمجيات المستخدمة في ذلك، كما يجب أن تتضمن إجراءات الطوارئ كيفية اللجوء إلى البديل اليدوي إذا تعذر استعادة البيانات إما بسبب تدمير النسخة الاحتياطية أو فشل البرمجيات المستخدمة في النسخ الاحتياطي في التوافق مع الأجهزة المتوافرة في الموقع البديل.

١-٤-٣- الأفراد

لابد أن تتضمن إجراءات الطوارئ وسيلة نقل الأفراد إلى الموقع البديل في أسرع وقت، ولابد أن تتوفر قوائم بخبرات أو مهارات بديلة من خارج المؤسسة يمكن اللجوء إليها في حالة قضاء الكارثة على المهارات والخبرات المحلية، لا قدَّر الله، ولا يقتصر الأمر على موظفي الحاسب فقط فإذا كانت هناك حاجة للجوء إلى البدائل اليدوية فلابد أن يتم استدعاء ونقل موظفي الإدارات المستفيدة، ويجب جدولة هذه الإجراءات حتى يمكن تحديد الوقت الذي ستبدأ فيه الخدمة البديلة، ولابد كذلك من وجود قوائم بأسماء وعناوين وهواتف هؤلاء الموظفين ، كما يجب أن تكون هناك قائمة محفوظة بأرقام المستفيدين الاحتياطية وكلمات المرور المرافقة.

١-٤-٤- التسهيلات الإضافية

تتضمن التسهيلات الإضافية التي تحتاج إليها فرق الطوارئ عند وقوع الكارثة ما يلي:

- خدمات النقل اللازمة لنقل الأجهزة والأفراد ووسائط تخزين البيانات ويجب أن يكون حجم ونوعية هذه الخدمات مناسبًا لما هو مطلوب منها.
- أجهزة الاتصالات وخدمة الهاتف التي يعتمد عليها في تنفيذ كثير من إجراءات الطوارئ.
- الشبكات ووسائل تبادل البيانات مع فروع المؤسسة.
- الكهرباء والمياه والمجاري سواء في الموقع المتضرر أو الموقع البديل بما في ذلك الاستعداد لتأمين وحدة توليد طاقة متنقلة إن لزم الأمر.
- الأثاث والأدوات المكتبية والأقراص والأشرطة الممغنطة والنماذج المطبوعة وباقي مستلزمات التشغيل.

١-٥- تشغيل الموقع البديل

يتم اللجوء إلى هذه الخطوة في حالة استحالة تشغيل الموقع الأصلي بعد الكارثة وتتضمن الخطوات التالية:

١) تشغيل الأجهزة بعد استكمالها.

٢) تحميل نظام التشغيل والبرمجيات المرافقة.

٣) إعادة تحميل البيانات من وسائط التخزين الاحتياطية.

٤) إدخال التعديلات اللازمة على رموز المستخدمين وكلمات المرور وباقي جداول النظام لتعكس البيئة الجديدة.

٥) تحميل التطبيقات الحرجة فقط دون غيرها.

٦) اختبار التشغيل في البيئة الجديدة وحل المشكلات التي قد تظهر.

٧) تحديث الملفات لتجاوز فترة التوقف، وتتوقف المدة اللازمة لإتمام هذه الخطوة ودرجة تكامل البيانات بعد إتمامها على درجة حداثة النسخ الاحتياطية للبيانات ومدى سلامة إجراءات استعادة النشاط بالنسبة لنظام الاتصال المباشر ونظام قواعد البيانات ، والجهات التي تستخدم نظم قواعد البيانات تكون لديها فرصة أفضل لتكامل البيانات نظرًا لوجود معظم البيانات في وعاء واحد (قاعدة البيانات) مما يضمن عدم ظهور اختلافات بين الملفات المختلفة.

٨) يتم بالتدريج إتاحة الخدمة المؤقتة للمستفيد مقتصرة على التطبيقات الحرجة فقط، ويتم مراقبة تقدم هذه العملية بدقة ومتابعة حل أي مشكلات قد تواجهها.

١-٦- إعادة الخدمة المعتادة للمستفيد

من المتفق عليه أن الموقع البديل هو موقع مؤقت ولابد أن يعود التشغيل إلى الموقع الأصلي بأسرع وقت، ويتطلب ذلك إصلاح الأصول المتضررة ويسبق ذلك فحص هذه الأصول لتحديد مدى الضرر الذي أصابها ومدى الإصلاح المطلوب الذي يتراوح بين مجرد التنظيف والاستبدال الكامل، وربما احتاج الأمر إلى إعادة تشييد أجزاء من المبنى، ويلزم بعد ذلك تقدير الزمن اللازم لاستعادة هذه الأصول لما كانت عليه ، ويتضمن ذلك الوقت اللازم لشراء أجهزة بديلة لتلك التي أصابها التلف وإعادة تركيب نظم التشغيل والبرمجيات.

يلزم بعد ذلك إعادة استخدام الموقع الأصلي، وهذه العملية تكون أقل استعجالاً من عملية تشغيل الموقع البديل ويمكن أن تتم ببطء وثقة. وعادة يتم إدخال واختبار التطبيقات غير الحرجة أولاً إلى الموقع الأصلي (على العكس مما كان عليه الحال في تشغيل الموقع البديل) وحل المشكلات التي قد تواجه هذه التطبيقات، وفي النهاية يتم نقل التطبيقات الحرجة واختبارها. وعادة تواجه مراكز الحاسب الآلي في هذه المرحلة مشكلة الكميات المتراكمة من البيانات المطلوب إدخالها ومعالجتها، ويتوقف ذلك بالطبع على مدة التعطل.

٢- مهام المشاركين في فرق الطوارئ

يجب أن يضم فريق الطوارئ في عضويته ممثلين عن كافة الإدارات المستفيدة بالمؤسسة بالإضافة إلى ممثلي إدارات مركز المعلومات بأكملها، ومن الضروري تمثيل الإدارة العليا في هذا الفريق، ويعين للفريق رئيس ونائب للرئيس كما يقسم إلى مجموعات عمل، ويتوقف عدد المشاركين في الفريق على حجم المؤسسة.

لابد أن يتلقى أفراد فريق الطوارئ في بداية عملهم تدريبًا مكثفًا لتزويدهم برؤية شاملة لعملية تحليل الأخطار وخطة الطوارئ، وبصفة عامة فهو يتشكل على النحو التالي:

٢-١- رئيس الفريق

يجب أن يكون رئيس فريق الطوارئ شخصًا ذا مركز متميز في المؤسسة يتمتع بثقة الإدارة العليا وقادرًا على إيجاد صلات وثيقة وفعالة مع مختلف المستويات بالمؤسسة، كما يجب أن يتمتع بمواهب تنظيمية وإدارية جيدة، وأن يكون على دراية كبيرة بالمؤسسة وأهدافها وخططها وأسلوب عملها وموظفيها، ويشرف رئيس الفريق على كتابة واختبار وصيانة خطة الطوارئ ثم نشرها وتوزيعها على من يلزم وضمان تحديث نسخ الخطة باستمرار، والإشراف على تدريب الفرق المشاركة في الخطة.

٢-٢- نائب الرئيس

يجب أن يتمتع بمعظم المزايا التي يتمتع بها الرئيس إضافة إلى النشاط وسرعة التفكير وحسن التصرف إذ إنه في كثير من الأحيان سيتولى بنفسه إدارة فريق الطوارئ، ففي معظم المؤسسات تسند رئاسة الفريق إلى شخصية مرموقة في المؤسسة، ليكون وجوده دافعًا لاتخاذ المؤسسة القرارات المهمة لدعم خطة الطوارئ، بينما يُسند العمل الفعلي لنائب الرئيس وبخاصة أثناء حدوث الكارثة.

٢-٣- مهام الفريق

١) تقويم الأخطار:

إعداد إجراءات تقويم الأخطار مع توضيح كيفية تحديد نوع الخطر وحجمه وكيفية اختيار البدائل الاحتياطية المناسبة.

٢) **التدابير المادية:**

وضع التدابير المادية لحماية الأجهزة والبرمجيات مثل: التحكم في دخول الأفراد، وأسلوب تخزين وسائط البيانات، وعمليات النقل، وأسلوب تجهيز الموقع البديل.

٣) **التدابير المنطقية:**

وضع التدابير المنطقية اللازمة لحماية النظام مثل: تأمين نظم التشغيل والبرمجيات والتطبيقات وقواعد البيانات وشبكات الاتصال وإجراءات ومعايير اختبار البرامج وتعديلها، وزمن الأداء المقبول، ومعايير التوثيق، وغير ذلك.

٤) **إعداد خطة الطوارئ:**

إعداد الإجراءات الواجب اتباعها في حالة وقوع الكارثة التي قد ينشأ عنها تدمير أصول المؤسسة الحساسة وكيفية مواجهة الطوارئ واستعادة النشاط.

٥) **قواعد توظيف الأفراد:**

وضع الإجراءات المناسبة التي تمر بها عملية التوظيف وتدريب الأفراد وقواعد استخدامهم لأصول المؤسسة وكيفية إنهاء عقود الأفراد سواء من جانب الفرد أو من جانب المؤسسة.

٦) **خطة التدريب:**

إعداد خطة تدريب الموظفين وأعضاء الفريق بما في ذلك الدراسات والندوات والحلقات التدريبية على كل مستويات المؤسسة حتى الإدارة العليا، وتحديد أسلوب التمهيد لتطبيق التدابير الأمنية بدلاً من مفاجأة الموظفين بتطبيقها.

٧) **الجودة النوعية:**

تحديد إجراءات الجودة النوعية والتأكد من أن نظم التطبيقات الجديدة تتضمن التدابير الأمنية اللازمة.

٨) **النواحي القانونية:**

إجراء تقويم شامل للقوانين الحالية والمرتقبة فيما يتعلق بأمن المعلومات سواء على مستوى المؤسسة أو الدولة بما في ذلك مراجعة بنود وثائق التأمين على الأجهزة والبرمجيات والأفراد.

٣- اختبار وصيانة ومراقبة خطة الطوارئ

٣-١- اختبار الخطة

خطة الطوارئ المفصلة هي محصلة عمل مجموعة كبيرة من الأفراد، وبالتالي فمن المحتمل أن يظهر فيها بعد اكتمالها أخطاء أو تضارب أو نقاط ضعف لم تؤخذ في الاعتبار ، ربما اعتمد طرف بشأنها على طرف آخر، ونقاط الضعف هذه لا تظهر للعين للوهلة الأولى وإنما سوف تظهر عند التطبيق..ولذلك تظهر الحاجة إلى اختبار الخطة ومراجعتها ومن ثم صيانتها لتنفيذ التعديلات المطلوبة، وهذه التعديلات قد لا تقتصر على أنشطة الحاسب الآلي فقط بل قد تمتد إلى أنشطة المؤسسة ذاتها.

٣-٢- معدل إجراء الاختبار

تتم بعض هذه الاختبارات بصفة دورية منتظمة بينما يُجرى بعضها الآخر بشكل عشوائي مفاجئ للتأكد من اتباع الإدارات لخطة الطوارئ بشكل

سليم. ويتولى فريق الطوارئ إجراء هذه الاختبارات ومن ثم يضع البرنــامج الزمني لصيانة الخطة بحيث يطلب من الجهات المطلوب مراجعة إجراءاتــها تنفيذ التعديلات المطلوبة في فترة زمنية محددة.

تخضع هذه الاختبارات لحساب التكلفة والعائد فهي تتكلف وقتًا ومــالاً وتأخذ من إمكانيات الحاسب والأفراد، ولكن هذه التكلفة تصبــح مقبولــة إذا قورنت بما قد تتكلفه المؤسسة إذا وقعت الكارثة وتبين عند ذلك أن الخطة لا تعمل بالشكل المطلوب.

٣-٣- نتائج الاختبار وصيانة الخطة

عند إجراء الاختبار يجب أن تكون الأخطار معروفة ومحــددة حتــى يمكن تصميم الاختبارات اللازمة لتحديد درجة التعرض، وقد تُظهر نتيجــة الاختبارات أخطارًا جديدة لم تكن معروفة من قبل مما يتطلب تعديل خطــة الطوارئ (صيانتها).

يشارك في اختبار الخطة موظفون من داخل المؤسسة أو متخصصون في أمن المعلومات من خارج المؤسسة ممن يســتطيعون بخبرتــهم إجــراء الاختبارات المفيدة التي تكشف أوجه النقص في إجراءات تأمين المؤسسة.

يجب الإعداد جيدًا للاختبار وصرف وقت كاف في هذا الإعــداد لأن الاختبار سيكون مكلفًا وربما قد ينتج عنه أعطال بالنظــام (وهــي أعطــال محكومة بالطبع)، كما يجب التأكد من أن الأفراد قد تم تدريبهم بشكل جيــد وإعلامهم بما هو متوقع. ومثلما يحدث في اختبار النظم الجديدة يتم اختبــار أجزاء الخطة كلاً على حدة ثم يتلو ذلك اختبار متكامل للخطة بأكملها للتــأكد من تناغم هذه الأجزاء مع بعضها، ويلاحظ هنا أنه لا يوجد فشل فــي هــذا الاختبار؛ فإذا فشلت مرحلة من المراحل فهذا يعد نجاحًا في حد ذاتــه لأنــه كشف ثغرة ما في الخطة سيتم معالجتها لاحقًا.

٣-٤- العوامل التي يجب أخذها في الاعتبار

فيما يلي بعض العوامل التي يجب أخذها في الاعتبار في مجال اختبار الخطة وصيانتها ومراقبتها:

١) يجب ألا يقل معدل إجراء الاختبارات عن مرتين في السنة.

٢) يجب أن تشمل الاختبارات أكبر عدد من الموظفين (ولو بالتناوب) لأن الاختبار يعني المزيد من التدريب ويمنح الموظف الثقة بالنفس وهو ما يحتاج إليه عند حدوث الكارثة الحقيقية.

٣) أبسط طرق الاختبار هي إعلان توقف الحاسب عن العمل ثم مراقبة الخطوات التي يتم اتباعها لإعادته إلى العمل، وهذا الأسلوب بالإضافة إلى بساطته فهو أقل الأساليب كلفة وأقدرها على اكتشاف الثغرات لتلافيها فيما بعد.

٤) قد يرفض المسئولون عن توفير الخدمة الاحتياطية نقل الأجهزة إلى الموقع المتضرر لمجرد إجراء اختبار، وهنا يجب أن تتسم الخطة بالمرونة، فيمكن الاستعاضة عن ذلك بنقل المستفيدين إلى موقع الخدمة الاحتياطية كبديل لغرض الاختبار.

٥) قد يكون من الصعب اختبار صلاحية الموقع البديل غير الفوري (Cold site) فتجهيزه مكلف ويستغرق وقتاً، ولكن يمكن الانتقال إلى موقع كامل مشابه ومحاكاة ظروف التشغيل المفروض حدوثها بعد استكمال الموقع البديل غير الفوري.

٦) يجب تسجيل نتائج الاختبارات وما يحدث خلالها بالضبط في ملحق من ملاحق خطة الطوارئ وتسجيل الإجراءات التي تم اتخاذها لمعالجة الأخطاء التي قد تقع خلال هذه الاختبارات، وفي العادة يتولى رئيس فريق الطوارئ أو نائبه تسجيل قائمتين لنقاط القوة والضعف في الخطة من واقع التطبيق العملي، وتُستخدم هاتان القائمتان في مرحلة مراجعة الخطة وتحسينها.

٧) من المهم أن تشارك الإدارة العليا في مراجعة الخطة بإقرار الحقائق الأولية مثل تحديد مصادر الخطر، وإقرار الإجراءات الأساسية للطوارئ مثل تحديد مستوى الموقع البديل. ويجب أن تتم هذه المراجعة عند انتهاء كل مرحلة من مراحل إعداد الخطة حتى لا يتسبب التعديل في إعادة تصميم أجزاء كبيرة من الخطة.

٤- تدريب الموظفين على تنفيذ الخطة

٤-١- نطاق التدريب

يجب أن تشمل خطة التدريب جميع الموظفين على كل مستويات المؤسسة حتى الإدارة العليا بالإضافة إلى التدريب الخاص المطلوب لأعضاء الفريق، ويختلف مستوى التدريب ومدته ونوعيته من فرد إلى آخر.

٤-٢- وسائل التدريب

١) الدراسات.

٢) الندوات.

٣) الحلقات التدريبية.

٤) الدوريات المنشورة.

٥) الأفلام التدريبية.

٤-٣- أهمية التدريب

تكمن أهمية التدريب في النقاط التالية:

١) أن يتعرف كل موظف بدقة على دوره خلال المراحل المختلفة من الخطة.

٢) أن يتعود الموظف على أسلوب تطبيق التدابير الأمنية بدلاً من مفاجأة الموظفين بتطبيقها.

٣) أن يتم تطعيم الموظف ـ من خلال التدريب ـ بحيث يتعود على التصرف لحظة وقوع الكارثة دون تردد أو هلع.

الفصل التاسع

تشفير البيانات (تعميتها)

موضوعات الفصل:

(١) مفهوم التشفير (التعمية) وتاريخه.
(٢) أهمية التشفير كوسيلة لتأمين البيانات.
(٣) شفرة "قيصر" (المفتاح السري).
(٤) نظام DES للتشفير.
(٥) التشفير باستخدام المفتاح العلني.
(٦) نظام RSA للتشفير.
(٧) التشفير المودع.



نتحدث في هذا الفصل عن أهم وسائل أمن المعلومات وأكثرها فاعلية، ألا وهو التشفير (أو التعمية)، نبدأ الفصل بتوضيح تاريخ التشفير في العصور القديمة ونصنف أنواع التشفير، ثم نتحدث عن أهمية التشفير كوسيلة لأمن البيانات.

ننتقل بعد ذلك إلى الحديث عن أساليب التشفير، فنبدأ بأسلوب التشفير باستخدام المفتاح السري "شفرة قيصر" ومزاياه وعيوبه وما تطور إليه هذا الأسلوب حاليًا، وكيفية كسر هذا النوع من التشفير. ثم نتحدث عن أحد أنواع هذا الأسلوب وهو أسلوب (تشفير البيانات القياسي DES)، ونشأته ونظرية عمله، ثم نقيم هذا الأسلوب موضحين كيفية تقييم أساليب الشفرة بصفة عامة والعوامل التي تؤخذ في الاعتبار عند التقييم ، ثم نبين كذلك كيف يمكن كسر شفرة هذا النوع من التشفير.

نقدم بعد ذلك أسلوب التشفير باستخدام المفتاح العلني وهو أكثر أساليب الشفرة شيوعًا الآن وأكثرها مقاومة للكسر، فنشرح كيفية عمله، ونشرح أسلوب التوقيع الرقمي المبني عليه، وتطبيقًا لأسلوب التشفير العلني نقدم نظام (RSA) للتشفير وأسلوب عمله. ثم نتحدث عن أسلوب التشفير "المودع" وكيفية عمله، وكيفية فك شفرة الرسائل عند الحاجة لذلك بواسطة رجال الشرطة، ثم نقدم تقييمًا واقعيًا لهذا الأسلوب من أساليب التشفير (التعمية).

١- مفهوم التشفير (التعمية) وتاريخه

١-١- مفهوم التشفير (Encryption)

بفرض أن لدينا رسالة نود إيصالها إلى شخص ما ولكننا نخشى من وقوع رسالتنا هذه في يد طرف ثالث لا ينبغي أن يطلع عليها. في هذه الحالة نقوم "بتعمية" الرسالة (لفظ التعمية هو اللفظ العربي القديم المستخدم للتعبير عن الرسائل المشفرة) بحيث لو تم اعتراض الرسالة المنقولة فلا ينكشف

مضمونها. هذا باختصار هو (التشفير Encryption) وهو وسيلة الحفاظ على أمن المعلومات في بيئة غير آمنة.

ربما كان التشفير هو أهم حجر في بناء أمن المعلومات ولكنه ليس الحجر الوحيد على أية حال. ويقول "بوير" أن أكثر وسائل أمن المعلومات فعالية هي "التشفير" ويعرفه على النحو التالي: (تشفير المعلومات هو تغيير مظهرها بحيث يختفي معناها الحقيقي) [Bowyer 1996]. فعن طريق تحوير صورة البيانات، بحيث تكون غير مفهومة لمن يتلصص عليها، يستطيع إخصائيو أمن المعلومات منع الأشخاص غير المرخص لهم من الاطلاع على هذه البيانات، وبذلك يحقق التشفير سرية البيانات. كما أن التشفير يمكن استخدامه بهدف تحقيق سلامة البيانات لأن البيانات التي لا يمكن قراءتها لا يمكن بالتالي تعديلها أو تزييفها. ويستخدم التشفير الآن كأساس لبعض البروتوكولات (مجموعة متتالية متفق عليها من الأفعال لتنفيذ مهمة معينة) التي تضمن إتاحة الموارد لمن يحتاج إليها.

يتضح من ذلك أن التشفير يقع في موقع القلب من وسائل ضمان أهداف أمن المعلومات الثلاثة التي سنتحدث عنها بالتفصيل في الفصل العاشر (نظم أمن البيانات) وهي: (خصوصية البيانات Data Confidentiality) و(سلامة البيانات Data Integrity) وإتاحة البيانات (Data Availability).

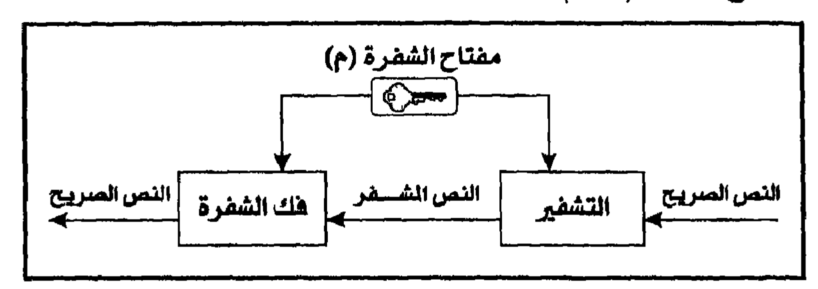
وبرغم أن التشفير يعتبر أداة هامة من أدوات أمن المعلومات إلا أننا يجب ألا نبالغ في هذه الأهمية، فالتشفير لا يحل جميع مشاكل أمن المعلومات. علاوة على ذلك فإذا لم يستخدم التشفير بالشكل المناسب، فقد لا يكون فعالاً في تأمين البيانات، أو قد يؤدي إلى سوء أداء النظام ككل. فالتشفير الضعيف يمكن أن يكون بالفعل أسوأ من عدم التشفير لأنه قد يعطي إحساسًا زائفًا بالأمن، لذلك فمن الأهمية بمكان أن نعرف المواقف التي يكون التشفير فيها مفيدًا وأن نستخدمه بكفاءة.

١-٢- أنواع التشفير

ينقسم التشفير بصفة عامة إلى نوعين أساسيين هما:

١) التشفير المتماثل:

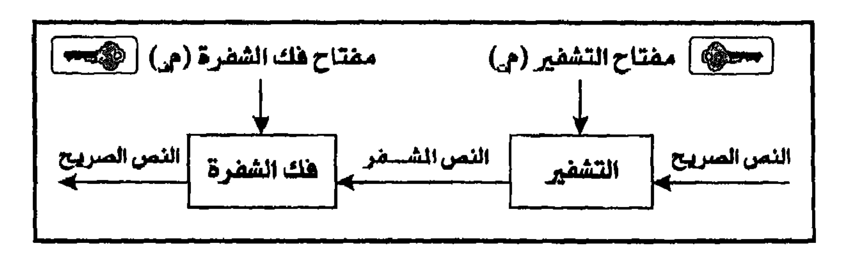
ويستخدم فيه مفتاح شفرة واحد لكل من عمليتي التشفير وفك الشـفرة، كما يوضح الشكل (٩-١).



شكل (٩-١) التشفير المتماثل

٢) التشفير غير المتماثل:

ويستخدم فيه مفتاحان للشفرة أحدهما يستخدم خلال عمليـة التشـفير والآخر يستخدم لفك الشفرة، كما يوضح الشكل (٩-٢).



شكل (٩-٢) التشفير غير المتماثل

٢- أهمية التشفير كوسيلة لتأمين البيانات

٢-١- الأخطار التي يمكن التغلب عليها بواسطة التشفير

يستخدم التشفير للتغلب على الأخطار التالية:

١) الاطلاع على المعلومات المحظورة.

٢) محاولات تعديل البيانات المنقولة بالشبكة.

٣) إعادة توجيه البيانات إلى وجهة أخرى.

٤) تأخير إيصال بعض الرسائل.

٥) تغيير محتويات الرسائل المتبادلة.

٦) إقحام رسائل زائفة ضمن الرسائل المنقولة عبر الخط.

٧) تغيير كلمات السر الخاصة بالمستفيدين.

٨) انتحال شخصية المستخدم الحقيقي.

٩) تعديل البيانات المخزنة على الحاسبات نفسها.

٢-٢- أساليب تشفير البيانات

هناك عدة أساليب لتشفير البيانات سنتعرض في هذا الفصل لأهم النماذج المتاحة منها مثل:

١) شفرة قيصر (المفتاح السري).

٢) نظام تشفير البيانات القياسي (Data Encryption Standard) أو (DES).

٣) التشفير باستخدام المفتاح العلني.

٤) نظام "RSA للتشفير" (Rivest, Shamir & Adleman).

٣- التشفير باستخدام المفتاح السري "شفرة قيصر"

٣-١- كيفية التشفير وفك الشفرة

من أقدم أساليب التشفير التقليدية أسلوب استخدام "المفتاح السري" (Private Key)، وأحيانًا يطلق عليه "المفتاح الوحيد" أو "المفتاح الخاص" وفي هذه الطريقة يتم تشفير المعلومات عن طريق "خوارزمية" (Algorithm) معينة باستخدام مفتاح شفرة معين. وسُميت باسم "قيصر" نسبة للإمبراطور الروماني "يوليوس قيصر" الذي استخدم هذا الأسلوب في تأمين رسائله إلى قادة جيوشه خلال فتوحاته الكثيرة.

فكرة التشفير باستخدام المفتاح السري (Private Key Encryption) يمكن أن تتضح من خلال مثال بسيط لشفرة "الاستبدال" التي تقوم على أن نستبدل بكل حرف من الأبجدية حرفًا آخر وفقًا لمفتاح شفرة معين . فإذا كان مفتاح الشفرة هو (٤) فمعنى ذلك أننا نضع مكان كل حرف في الرسالة الحرف الذي يليه في الأبجدية بأربعة أحرف. وعندما نصل إلى نهاية الأبجدية "حرف الياء" نعتبر الحرف التالي له هو بداية الأبجدية "حرف الألف" أي تصبح الحروف حلقة متصلة. ونفترض أن المسافة الخالية " " تأتي بعد حرف الياء، وبذلك يكون جدول التشفير كالتالي:

ا	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي	
ج	ح	خ	د	ذ	ر	ز	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي		ا	ب	ت	ث

جدول (٩-١) جدول استبدال بسيط

وبذلك إذا أردنا تشفير الرسالة التالية:

(الاجتماع السري سيكون موعده يوم الاثنين)

تصبح الرسالة المشفرة هي:

(جوجذخيجكثجوطصتتطتهب ثيبكساثتبيثجوجد ت).

لتشفير أي رسالة بهذا النظام يلزم معرفة كل من الخوارزمية (التي كانت هي الاستبدال في المثال السابق) ومفتاح الشفرة (الذي كان هو الرقم ٤ في المثال السابق). أما حل الشفرة فهو بكل بساطة مجرد عكس الإجراء السابق لإعادة الحروف إلى ما كانت عليه.

في التطبيق العملي لهذا الأسلوب من التشفير على شبكات الحاسب يتم اختيار خوارزمية قياسية تكون معلومة للجميع، وبذلك تعتمد سرية النص المشفر على معرفة المتلقي (وحده) لمفتاح التشفير، ويضفي ذلك أهمية كبيرة على ضرورة إبقاء مفتاح التشفير سرًا، ولذلك سُمي "المفتاح السري". ومادام إرسال مفتاح الشفرة عبر نفس شبكة الاتصال قد يعطي الآخرين فرصة معرفة المفتاح فلابد من تبادل مفتاح الشفرة السري عن طريق آلية آمنة أخرى خارج الشبكة.

٣-٢- عيوب التشفير باستخدام المفتاح السري

يتضح مما سبق أن استخدام "الاستبدال" كخوارزمية للتشفير هو أسلوب بسيط يسهل كسره، إذ إن الشخص المتلصص يكفيه أن يحصل على نسخة من الرسالة المشفرة، وبإجراء عدة محاولات بالتباديل والتوافيق للقيم المختلفة الممكنة لمفتاح الشفرة حتى يحصل على نص مفهوم، يمكنه استنتاج قيمة مفتاح الشفرة الصحيح. وهذا الأسلوب لكسر الشفرة لا يستغرق سوى دقائق قليلة، وبمجرد معرفة خوارزمية التشفير هناك كذلك فرصة لاستخدام أسلوب البحث العشوائي عن المفاتيح المحتملة. ولعلاج هذه المشكلة، إلى حد ما، يمكن زيادة احتمالات تكوين المفتاح إلى الحد الذي يجعل الوقت المطلوب لكسر النص المشفر يمتد ليصبح مئات السنين!!

ولكن الأمر للأسف ليس بهذه البساطة فالمتلصص يمكنه استخدام خصائص معينة في خوارزمية التشفير المستخدمة لخلق أسلوب بحث أكثر فعالية. ولذلك يُطلق على بعض أساليب التشفير وصف "تشفير ضعيف" أو "تشفير قوي" تبعًا للوقت المطلوب لكسر النص المشفر. ولهذا النظام بعض العيوب الأساسية التي تحد إلى حد كبير من فائدة هذا النوع من التشفير وهي:

١) ضرورة توزيع المفتاح السري على جميع الأشخاص الذين تكون هناك حاجة للتراسل معهم.

٢) عدم وجود وسيلة حاسمة لتحديد شخصية مرسل الرسالة والتأكد من أن الرسالة لم تتعرض للتعديل من قبل شخص آخر.

٣) بالنظر إلى نتيجة التشفير (النص المشفر) يمكن أن نستخرج من النص الصريح علامات تضيء الطريق، مثل: الفواصل بين الكلمات، أو بعض الحروف التي تبدأ بها الكلمات مثل حرفي "ألف لام"، أو بعض

الحروف التي تنتهي بها الكلمات مثل "هم" و"ها" والتاء المربوطة وغير ذلك، أو الكلمات التي يكثر عادة تداولها ضمن الرسائل مثل "في" و"على" و"من"، أو بعض الأرقام مثل التاريخ، أو ربما عبارات كاملة مثل "السلام عليكم ورحمة الله وبركاته" في بداية الرسالة أو "وتفضلوا بقبول وافر الاحترام" في نهايتها. هذه العلامات المضيئة تجعل الرسالة بل والشفرة نفسها سهلة الكسر.

فلكسر الشفرة المذكورة في المثال السابق نبدأ بدراسة النص المشفر فنجد أن حرفي الجيم "ج" والواو "و" يتكرران معًا أكثر من مرة، ونكتشف أن المسافة بينهما في الأبجدية هي نفس المسافة بين حرفي الألف "أ" واللام "ل"، وهذا وحده يكفي لكسر الشفرة كلها، كما نجد أن حرف الثاء "ث" يتكرر على مسافات تتراوح بين ثلاثة إلى ثمانية حروف مما يجعلنا نشك أن هذا الحرف يمثل المسافة الخالية.

٣-٣- محاولات تحسين شفرة قيصر

أُجري على هذا النوع من التشفير تطوير ألغيت بمقتضاه المسافات تمامًا لأنه من المفترض أن المتلقي المقصود بالرسالة في مقدوره أن:

(يستطيعتقطيعالنصالصريحللرسالةإلىكلماتدونعناء).

ثم خضع هذا الأسلوب إلى تطوير آخر ، وهو تقسيم النص المشفر إلى أجزاء متساوية بغض النظر عن أماكن وجود المسافات فتكون الرسالة، طبعًا بعد تعديل الجدول بإلغاء المسافة، شيئًا كهذا:

(جوجذ خيجك جوطص ثطثه تايت كسبث تيجو جداث أ)

واستمر تحسين هذا النوع من التشفير فلم يعد تحوير الحروف (أن يأخذ كل حرف قيمة حرف آخر) يتبع أسلوب استبدال بسيط كأن نستبدل به الحرف الذي يليه في الأبجدية بسبعة أو تسعة أحرف، ولكن في هذه الحالة يتم اختيار الحرف المقابل وفقًا لقاعدة أكثر صعوبة كأن يكون الحرف المقابل لحرف الألف هو الحرف الذي يليه مباشرة والحرف المقابل لحرف الباء هو الحرف الذي يليه بحرفين والحرف المقابل لحرف التاء هو الحرف الذي يليه بثلاثة أحرف، ثم نعود من البداية أي إن الحرف المقابل لحرف الثاء هو الحرف التالي أي حرف الجيم، وهكذا. ولكي نتفادى تكرار الحروف نكمل الأبجدية إلى ثلاثين حرفًا بإضافة علامتي الاستفهام والتعجب مثلاً، أي يكون لدينا جدول تشفير كالجدول التالي:

ا	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	ه	و	ي	؟	!
ب	ث	ح	ج	خ	ذ	د	ر	س	ز	ش	ض	ص	ط	ع	ظ	غ	ق	ف	ك	م	ل	ن	و	ه	ي	!	؟	أ	ت

جدول (٩-٢) جدول استبدال أكثر تعقيدًا

٣-٤- كيفية كسر شفرة قيصر

تتم الاستعانة بجداول تكرارات الحروف وهي جداول يتم تكوينها من قواميس اللغة ومن العديد من النصوص المكتوبة بهذه اللغة لتحديد احتمالات ورود حرف اللام بعد حرف الألف مثلاً واحتمالات ورود حرف الألف بعد حرف اللام، وهكذا يوجد لكل حرف بالأبجدية جدول (ثنائيات Digrams) يبين النسبة المئوية لورود جميع الحروف قبله أو بعده كالجدول التالي:

	أ	ب	ت	ث	..
أ	٢	٣٠	١٢	٤	
ب	٢٠	٧	٩	١	
ت	١٨	١١	٥	٢	
ث	٥	٤	١	٠	
..					

(الأرقام في الجدول السابق تمثل النسبة المئوية لورود حرف معين تاليًا لحرف آخر)

جدول (٩-٣) مثال لجدول (الثنائيات Digrams) لحروف اللغة العربية

بالنظر إلى الجدول السابق (وهو ليس جدولاً حقيقيًا، وإنما أوردناه لأغراض الشرح فقط) نجد أن احتمال ورود حرفي الألف متتاليين هو ٢% بينما احتمال ورود حرف الباء بعد حرف الألف هو ٣٠% واحتمال تكرار حرفي الثاء هو صفر%، وبذلك يمكن ترجيح احتمال ورود حرف على احتمال ورود حرف آخر وفقًا لجداول الثنائيات (Digrams) هذه. وتوجد جداول من هذا النوع لكل لغة من اللغات بما في ذلك اللغة العربية، ويبين الجدول (٩-٤) جدول الثنائيات للغة الإنجليزية [Pfleeger 1997].

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	0.0	19.2	41.3	11.4	0.1	3.7	10.2	0.6	13.9	0.6	4.7	70.7	19.0
B	5.6	0.0	0.0	0.1	35.7	0.0	0.0	0.0	7.0	13.1	0.0	19.8	0.4
C	42.5	1.6	15.1	0.1	56.1	0.1	0.0	37.1	14.5	0.0	5.9	10.3	0.0
D	11.7	0.1	0.0	3.4	73.6	0.0	0.8	0.0	26.7	0.0	0.0	0.8	0.6
E	39.3	0.5	80.9	70.4	16.1	12.9	8.6	0.6	5.9	0.1	0.3	41.2	37.8
F	8.6	0.0	0.0	0.0	17.7	14.2	0.0	0.0	25.5	0.0	0.0	3.8	0.0
G	6.6	0.0	0.0	0.0	19.2	0.1	0.4	11.4	7.6	0.0	0.0	1.6	0.8
H	50.4	0.0	0.0	0.0	146.4	0.1	0.0	0.1	24.7	0.0	0.0	0.4	0.5
I	16.9	8.4	43.4	17.4	18.6	21.7	32.7	0.0	0.0	0.0	1.3	22.5	27.8
J	0.0	0.0	0.0	0.0	16.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
K	0.5	0.0	0.0	0.0	10.5	0.0	0.0	0.0	2.8	0.0	0.0	0.1	0.0
L	32.1	0.1	0.2	7.9	65.7	0.6	0.5	0.0	30.6	0.0	0.1	30.6	0.3
M	33.9	4.8	0.1	0.3	62.3	0.0	0.0	0.0	15.9	0.0	0.0	0.4	7.3
N	20.2	0.2	28.5	67.8	41.4	9.7	58.5	0.5	21.1	0.1	0.9	3.5	2.2
O	1.8	10.3	11.6	21.3	2.0	67.7	8.5	0.1	2.4	2.9	2.3	20.4	35.5
P	19.4	0.1	0.2	0.1	48.4	0.2	0.0	2.7	2.7	0.0	0.0	24.6	1.6
Q	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
R	52.0	0.1	12.4	7.8	132.3	3.0	5.1	0.3	75.2	0.0	2.7	2.4	18.6
S	8.1	0.0	7.8	0.2	97.2	1.8	0.0	10.2	52.5	0.0	1.7	1.4	4.2
T	37.5	0.0	3.8	0.2	101.5	0.3	0.0	196.8	121.0	0.0	0.0	2.7	4.4
U	16.8	8.3	13.5	7.7	9.9	0.5	3.6	0.0	6.9	0.0	0.0	24.4	6.1
V	17.0	0.0	0.0	0.0	51.5	0.0	0.0	0.0	20.3	0.0	0.0	0.0	0.5
W	12.6	0.0	0.1	0.0	19.2	0.0	0.0	16.2	16.7	0.0	0.0	0.2	0.0
X	6.4	0.0	0.3	0.0	1.9	0.0	0.0	0.1	1.8	0.0	0.0	0.0	0.0
Y	0.2	0.1	0.1	0.2	2.6	0.0	0.0	0.0	1.7	0.0	0.0	0.0	0.2
Z	3.2	0.0	0.0	0.0	4.6	0.0	0.0	0.0	0.3	0.0	0.0	0.0	0.0
Sp	201.1	60.0	98.4	65.4	63.9	64.0	12.4	27.8	120.7	2.2	7.1	31.4	58.2

الأرقام هي من بين كل ١٠,٠٠٠ حرف

جدول (٩-٤) جدول الثنائيات (Digrams) للغة الإنجليزية (٢/١)

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Sp
A	119.1	0.0	10.9	0.0	65.9	49.8	118.8	6.6	9.8	1.8	0.9	9.6	0.0	55.8
B	0.0	4.5	0.0	0.0	1.9	1.8	0.6	7.5	0.3	0.0	0.0	8.2	0.0	7.4
C	0.0	57.4	0.0	0.1	11.7	2.4	63.2	28.5	0.0	0.0	0.0	3.0	0.0	126.6
D	0.1	11.0	0.0	0.0	2.0	5.8	0.1	12.5	1.1	1.6	0.0	3.0	0.0	126.6
E	99.2	2.0	13.3	8.0	143.0	132.0	26.4	1.8	27.0	3.1	28.9	4.4	0.0	310.9
F	0.0	37.2	0.0	0.0	8.2	0.2	5.3	7.7	0.0	0.0	0.0	1.9	0.0	70.2
G	16.6	3.5	0.0	0.0	12.8	1.0	0.5	8.5	0.0	0.0	0.0	0.5	0.0	50.4
H	3.2	23.4	0.0	0.0	7.3	0.4	5.8	2.3	0.0	0.0	0.0	3.4	0.0	36.3
I	142.3	70.6	4.9	2.6	15.9	64.4	80.6	0.3	15.9	0.0	1.9	0.0	6.9	1.4
J	0.0	1.3	0.0	0.0	0.0	0.0	0.0	1.2	0.0	0.0	0.0	0.0	0.0	0.6
K	3.1	0.1	0.0	0.0	0.0	2.4	0.0	0.2	0.1	0.1	0.0	0.0	0.0	6.8
L	0.4	18.1	1.0	0.0	0.2	11.1	9.2	9.2	2.3	0.5	0.0	24.6	0.0	67.9
M	0.3	20.3	25.2	0.0	0.0	12.9	0.0	8.9	0.6	0.0	0.0	0.5	0.0	32.3
N	4.0	21.2	0.1	0.1	0.7	37.5	83.0	3.6	6.5	0.0	0.0	6.1	0.0	151.5
O	12.1	9.1	23.1	0.0	88.7	14.6	28.3	45.1	8.3	17.6	0.3	0.5	0.0	64.3
P	0.0	20.3	9.7	0.0	46.9	2.2	6.3	4.9	0.0	0.0	0.0	0.3	0.0	6.4
Q	0.0	0.0	0.0	0.0	0.0	0.0	0.0	14.8	0.0	0.0	0.0	0.0	0.0	1.0
R	5.7	62.1	2.1	0.0	5.9	21.5	20.3	11.9	5.6	0.3	0.0	10.7	0.0	94.0
S	0.5	23.6	7.4	0.1	0.1	43.7	77.9	30.7	0.0	2.6	0.0	21.1	0.0	257.8
T	0.7	60.4	0.5	0.0	31.9	38.3	4.4	14.3	0.0	10.9	0.0	34.2	0.2	137.7
U	18.6	0.5	6.0	0.0	53.7	43.9	16.9	0.0	0.0	0.0	0.1	0.1	0.1	13.3
V	0.0	2.8	0.0	0.0	0.0	0.5	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.1
W	3.4	10.4	0.0	0.0	1.6	2.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	10.2
X	0.0	0.1	16.5	0.0	0.0	0.0	2.1	0.0	0.0	0.0	0.0	0.0	0.0	3.6
Y	0.6	15.5	5.0	0.0	0.2	25.2	0.3	0.1	0.0	0.1	0.0	0.0	0.9	96.1
Z	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0
Sp	27.4	135.2	71.6	4.8	53.2	136.3	251.9	30.0	15.7	54.7	0.5	16.6	0.1	0.0

الأرقام هي من بين كل ١٠,٠٠٠ حرف

جدول (٩-٤) جدول الثنائيات (Digrams) للغة الإنجليزية (٢/٢)

ويمكن تطوير هذه الجداول لتكون ثلاثية الأبعاد لتبين احتمالات تكرار ثلاثة حروف متتالية وهي جداول (الثلاثيات Trigrams) أو أكثر من ذلك.

يبين الجدول (٩-٥) الحروف المتجاورة كثيرة الورود في اللغة الإنجليزية مثنى (ثنائيات Digrams) وثلاث (ثلاثيات Trigrams) .

DIGRAMS	TRIGRAMS
EN	ENT
RE	ION
ER	AND
NT	ING
TH	IVE
ON	TIO
IN	FOR
TF	OUR
AN	THI
OR	ONE

جدول (٩-٥) الثنائيات والثلاثيات الأكثر شيوعًا في اللغة الإنجليزية

وباستخدام جداول الثنائيات والثلاثيات وجداول التكرار يمكن فحص الحروف التي تتكون منها الرسالة لاستنتاج الحرف الأصلي في النص الصريح. ويحتاج الأمر إلى إجراء عمليات حسابية ومقارنات كثيرة ولكن باستخدام الحاسب الآلي أصبحت هذه العملية أكثر سهولة، فيمكن توليد آلاف الاحتمالات من النصوص في لحظات لاختبارها في محاولة للوصول إلى نص مفهوم. وحتى هذا الاختبار يمكن أن يتم آليًا بعرض هذه النصوص على

قاموس اللغة الآلي ليبين كم منها يمثل كلمات صحيحة، وكم منها يمثل كلمات لا وجود لها في القاموس، ويتم اختيار النص الذي به أكبر نسبة من الكلمات المفهومة بعد فك التشفير.

٣-٥- شفرة التحوير المزدوج

شفرة التحوير المزدوج تتضمن تبديلاً مزدوجًا للأعمدة، أي أن التبديل (التحوير) يتم على مرحلتين، ففي المرحلة الأولى يتم تقسيم النص إلى أعمدة فينتج عن ذلك فصل الحروف المتجاورة، وفي المرحلة الثانية يتم تكوين أعمدة جديدة بهدف كسر تجاور السلسلة القصيرة من الحروف التي يتصادف ظهورها في أعمدة متجاورة بعد تنفيذ التحوير الأول، ويبين الجدول (٩-٦) النص الصريح التالي بعد تقسيمه إلى أعمدة (التحوير الأول):

"This is a message to show how a columnar transposition works"

T	H	(I)	[S]	I
S	A	(M)	[E]	S
S	A	(G)	[E]	T
O	S	(H)	[O]	W
H	O	(W)	[A]	C
O	L	(U)	[M]	N
A	R	(T)	[R]	A
N	S	(P)	[O]	S
I	T	(I)	[O]	N
W	O	(R)	[K]	S

جدول (٩-٦) النص الصريح بعد تحوير الأعمدة الأول

قمنا بوضع حروف العامود الثالث بين قوسين دائريين ( ) وحـــــروف العامود الرابع بين قوسين مربعين [ ] وذلك لتسهل متابعتـــها فـــي النـــص المشفر، فيصبح النص المحور بعد أن نقرأ الأعمدة بشكل طولي هكذا:

TSSOH OANIW HAASO LRSTO (I)(M)(G)(H)(W) (U)(T)(P)(I)(R) [S][E][E][O][A] [M][R][O][O][K] ISTWC NASNS

ولأن النص الصريح كان مكونًا من ٥٠ حرفًا، فقد أمكـــن اســتيعابه بسهولة في مصفوفة أبعادها ١٠×٥ . والآن يأتي دور التحوير الثاني الـــذي يظهره الجدول (٩-٧) حيث تم وضع النص المشفر في مصفوفـــة أبعادهـــا ٨×٧ ، وتم الاحتفاظ بالأقواس لتسهيل تتبع الحروف في مواضعها الجديـــدة. ولأن الحروف الخمسين لا يمكن أن تملأ مصفوفة أبعادها ٨×٧ (٥٦ حرفًا) فيجب ملء المواضع الإضافية بأحد الحروف وليكن حرف (X) مثلاً ، ولكن من الناحية التطبيقية يراعى اختيار حروف مـــلء مـــن الحـــروف كثـــيرة الاستخدام مثل حروف A,E,I,O,N,S حتى لا يسهل اكتشافها.

T	S	S	O	H	O	A
N	I	W	H	A	A	S
O	L	R	S	T	O	(I)
(M)	(G)	(H)	(W)	(U)	(T)	(P)
(I)	(R)	[S]	[E]	[E]	[O]	[A]
[M]	[R]	[O]	[O]	[K]	I	S
T	W	C	N	A	S	N
S	X	X	X	X	X	X

جدول (٩-٧) النص الصريح بعد تحوير الأعمدة الثاني

وينتج عن التحوير الثاني للأعمدة النص المشفر التالي الذي يتضح منه كيف تمت بعثرة الحروف تمامًا:

TNO(M)(I) [M]TSSI L(G)(R)[R]W XSWR(H) [S][O]CXO HS(W)[E][O] NXHAT (U)[E][K]AX OAO(T)[O] ISXAS (I)(P)[A]SN X

ويمكن استخدام أي خوارزمية للتحوير بشرط أن تتبع قاعدة معينة ليمكن إعادتها إلى أصلها مرة أخرى عند فك الشفرة.

٤ - نظام (Data Encryption Standard DES) للتشفير

٤-١- نشأة النظام

أسلوب (تشفير البيانات القياسي Data Encryption Standard) أو (DES) يعتبر نوعًا من أنواع التشفير باستخدام المفتاح السري، وهذا الأسلوب طورته شركة "آي بي إم" للحكومة الأمريكية في منتصف السبعينيات من القرن العشرين [Bowyer-1996] ، ولكنه خضع لتعديلات كثيرة قبل أن تتم الموافقة على اعتماده في عام ١٩٧٧ من جانب الحكومة الأمريكية [Landau-1994a, Melford-1993] وأُخضع هذا النظام لمحاولات كسره باستخدام أسلوب (باب المصيدة Trapdoor) للكشف عن المفتاح السري، ولكن لم يمكن كسر النص المشفر بسهولة مما أوجد نوعًا من الإجماع على أن نظام (DES) يقدم أسلوب تشفير قوي نسبيًا وفقًا لما أورده "لاندو" منذ سنوات [Landau 1994a]. وعلى أي حال فقد ثبت أن تكرار

تشفير النص الصريح عدة مرات يمكن أن يؤدي إلى نتائج أفضل، ولذلك فإن هذا الأسلوب ظل لفترة طويلة أكثر أساليب التشفير انتشارًا في العالم [Bowyer 1996].

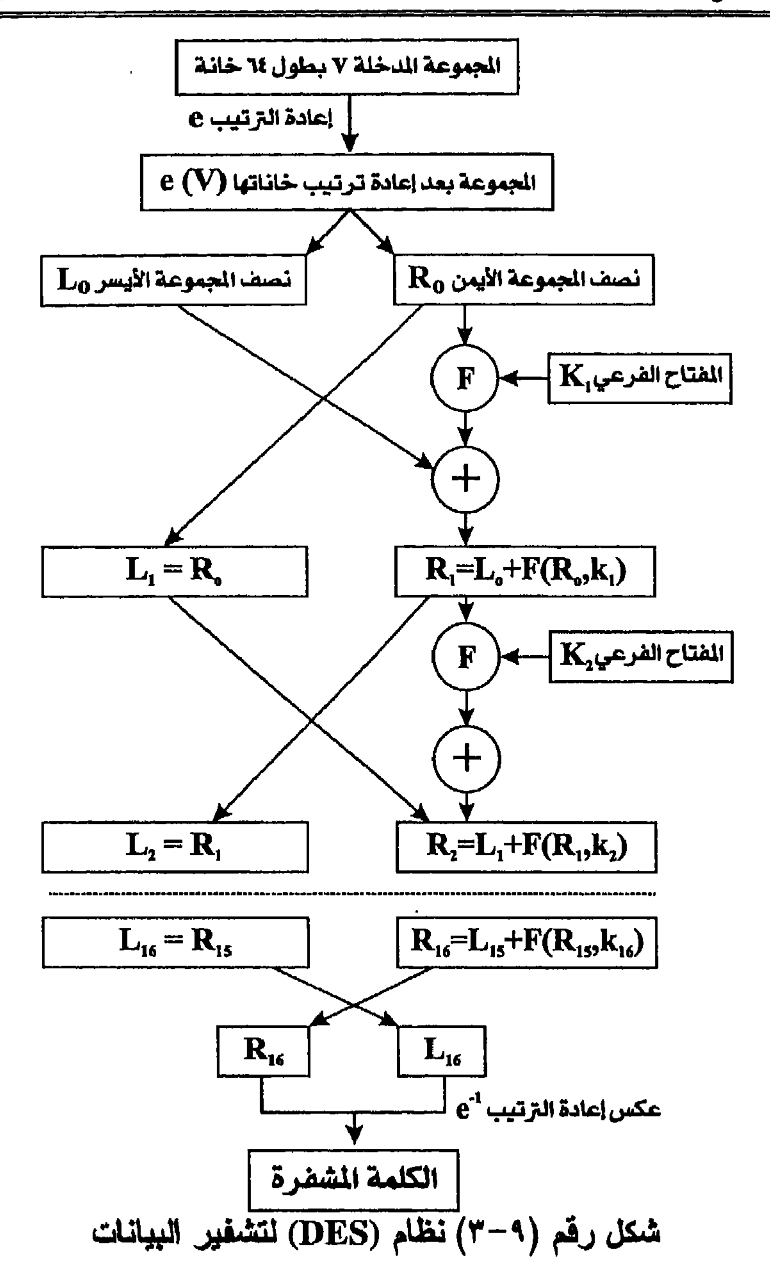
أصبحت برامج التشفير باستخدام هذا الأسلوب متاحة حتى على شبكة الإنترنت، ويؤكد "بارلو" أن الأمر الآن لا يستغرق سوى ثلاث دقائق وأربع عشرة ثانية للعثور على نسخة من النص الأصلي (Source Code) على شبكة الإنترنت [Barlow 1993]. وتحتاج بعض المنتجات التي تعتمد على هذا الأسلوب في التشفير إلى تصريح خاص من الحكومة الأمريكية عند تصديرها خارج الولايات المتحدة حفاظًا على الأمن القومي الأمريكي [Landau 1994a].

نظرًا لأن عملية البحث الآلي عن المفتاح لم تعد تستغرق وقتًا طويلاً هذه الأيام مع تقدم تقنيات الحاسب، فإن ذلك ينبئ بأفول شمس هذا الأسلوب من أساليب التشفير. الأمر الذي دعا إلى التفكير في أسلوب آخر أحدث وأكثر فاعلية مما سبقه من أساليب ألا وهو أسلوب (التشفير المودع Escrowed Encryption Standard) أو (EES) والذي سنفرد له قسمًا خاصًا في هذا الفصل.

٤-٢- كيف يعمل النظام؟

يعتمد هذا الأسلوب على تشفير مجموعات الحروف حيث يتم تقسيم النص المراد تشفيره إلى مجموعات حجم كل منها (٨) حروف أي (٦٤) خانة (bit) ويتكون مفتاح التشفير من (٦٤) خانة كذلك (منها ٥٦ خانة للتشفير وثماني خانات تستخدم للتدقيق parity). ويبين شكل رقم (٩-٣) كيف تمر خانات المجموعة المطلوب تشفيرها أولاً خلال عملية أولية تتضمن

إعادة ترتيب أماكن الخانات، ثم بعد ذلك يتم تقسيم المجموعة إلى نصفين (النصف الأيسر L_0 بحجم ٣٢ خانة، والنصف الأيمن R_0 بحجم ٣٢ خانة أخرى). ثم يتم توليد مفتاح تشفير فرعي حجمه (٤٨) خانة من مفتاح التشفير الرئيسي. وبعد ذلك يتم إدخال نصف المجموعة الأيمن R_0 في عملية تحويل رياضية F(R,KEY) باستخدام مفتاح التشفير الفرعي، وينتج عن هذه العملية مجموعة جديدة من الخانات (٣٢ خانة أيضًا) ثم يتم إجراء العملية المنطقية (Exclusive OR) بين هذه المجموعة الجديدة وبين النصف الأيسر من البيانات الأصلية (L_0) مما ينتج النصف الأيمن في صورته النهائية المشفرة (R_1). أما النصف الأيمن الأصلي R_0 فيتم نقله ليصبح هو نفسه النصف الأيسر في صورته النهائية المشفرة (L_1). ثم يتم تمرير النصفين الجديدين (L_1) و (R_1) معًا خلال عملية تحويل رياضية تتكرر (١٦) مرة بحيث في كل مرة يتم استخدام مفتاح تشفير فرعي مختلف متولد من مفتاح التشفير الرئيسي. في النهاية يتم إجراء عملية إعادة ترتيب جديدة على المجموعة الناتجة هي عكس العملية الأولى التي أجريت على المجموعة في البداية لتنتج في النهاية المجموعة المشفرة المكونة من (٦٤) خانة.



شكل رقم (٩-٣) نظام (DES) لتشفير البيانات

وعند إعادة التشفير يتم إعادة المجموعة إلى صورتها الأصلية، ولكن يلاحظ أنه إذا فقدت خانة واحدة أثناء نقل البيانات فإنه لن يمكن استعادة المجموعة التي تحتوي على هذه الخانة. ويعيب هذا الأسلوب أن كل مجموعة مستقلة تمامًا عن الأخريات، فلا يمكن اكتشاف فقدان أي مجموعة خلال عملية النقل.

ولإضفاء مزيد من التأمين على البيانات المنقولة يستخدم أسلوب مختلف وهو أسلوب (CBC) أو (Cipher Block Chaining). وفي هذا الأسلوب يتم تقسيم الرسالة ــ كما تقدم ــ إلى مجموعات متتالية حجم كل منها (٦٤) خانة، ثم يتم تشفير المجموعة الأولى باستخدام أسلوب (DES)، وقبل أن يتم تشفير المجموعة التالية تجرى العملية المنطقية (Exclusive OR) بينها وبين المجموعة الأولى (في صورتها المشفرة). ويتكرر ذلك بين كل مجموعة من مجموعات الرسالة والمجموعة السابقة لها وذلك حتى آخر مجموعة في الرسالة. ويمتاز هذا الأسلوب بأنه يلغي استقلالية المجموعات كما كان الحال سابقًا حيث يعتمد تشفير كل مجموعة على نتيجة تشفير المجموعة السابقة، ولكن ذلك يعني في الوقت نفسه أن فقدان خانة واحدة من أي مجموعة يؤثر على مجموعتين وليس على مجموعة واحدة، أي يعني فقدان (١٢٨) خانة. ولكن هذا الأسلوب في نهاية الأمر يزيد من تأمين البيانات إذ يمكن من اكتشاف ضياع أي مجموعة من البيانات أو تكرار إرسالها.

وعند إرسال البيانات باستخدام هذا الأسلوب يتم استخدام مفتاح شفرة معلوم لدى الطرفين (المرسل والمستقبل)، وليكن (K)، والذي يستخدم لتشفير مجموعة الخانات ثم تؤخذ الخانات الست عشرة اليمنى من المفتاح (K) لتجرى العملية المنطقية (Exclusive OR) بينها وبين رمز المستفيد للشخص المرسل (Personal Identification Number) أو (PIN) ويسمى الرمز

النـــاتج (Message Authentication Code) أو (MAC) وتتــم إضافتـــه للرسالة قبل إرسالها. وفي الطرف الآخر يقوم المستقبل (الذي يعرف كلاً من مفتاح الشفرة K ورمز المستفيد PIN) بإجراء نفس العملية المنطقية لإنتـــاج (MAC) ومقارنته بالقيمة الواردة مع الرسالة للتأكد من شخصية المرســـل، وهذه العملية برمتها تتم الآن آلياً. وكثيرًا ما يتم استخلاص الرمـــز (MAC) والذي ينتج من كل من محتويات الرسالة وبيانات المرسل ثم يضـــاف هـــذا الرمز للرسالة نفسها دون تشفير، وعند استقبال الرسالة يســـتطيع الطـــرف المستقبل إعادة توليد الرمز (MAC) لاكتشاف ليس فقط الطـــرف المرســـل ولكن أيضًا لاكتشاف وجود أي خطأ خلال عملية نقـــل البيانـــات، إذ إن أي خطأ في النقل سينتج عنه اختلاف الرمز (MAC).

٤-٣- تقييم أسلوب (DES)

تعرض هذا النظام لانتقادات كثيرة ظهر بعضها علنًـــا فـــي الكتـــب والمقالات، ولكن بعض خصائص النظام لم يتم الكشف عنها بعد من جـــانب المطورين، ولم يتمكن محللو نظم الشفرة أو المتخصصون في كسر الشفرات من الاطلاع على تفاصيلها [Pfleegr 1997]. وكثير من أجهزة الاستخبارات في دول كثيرة بالعالم ترغب في الاطلاع على التفاصيل العلمية الكاملة لـــهذا الأسلوب، وتتحرق إدارات كسر الشفرة في هذه الأجهزة شوقًا لمعرفة كـــل شيء عن أساليب التشفير المختلفة.

وسنقدم فيما يلي تقييمًا لبعض العناصر الأساسية التـــي تؤخـــذ فـــي الاعتبار عند تقييم نظم الشفرة:

١) تصميم الخوارزمية .

بعض عناصر التصميم الرئيسية اعتبرتـــها وكالـــة الأمـــن القومـــي الأمريكية من المعلومات الحساسة ومنعت نشرها، ومن بينها أسلوب التحوير

واشتقاق المفاتيح الفرعية، فقد كان هناك العديد من الخيارات المتاحة ولكن واحدًا منها فقط هو الذي تم اختياره للاستخدام في نظام (DES) ولذلك أُبقي هذا الخيار الاستراتيجي سرّا، وهذه السرية تثير المخاوف من زرع فيروس "باب المصيدة" ضمن الخوارزمية المستخدمة مما يجعل صانعيها قادرين بسهولة على فك شفرة أي رسالة يتم تشفيرها بواسطة هذا الأسلوب، مما يعطي وكالة الأمن القومي الأمريكية القدرة على انتهاك خصوصية ملايين الرسائل المتبادلة حول العالم بين الأفراد أو بين الحكومات أو بين الجيوش المتحاربة!!

بعد تحقيق طويل في الكونجرس الأمريكي (أُبقيت نتائجه سرية حتى الآن) تم إذاعة بيان مقتضب يبرئ وكالة الأمن القومي الأمريكية من أي تورط غير مشروع في تصميم خوارزمية (DES) [SMID 1988].

النقطة الثانية التي أثيرت حول هذا الأسلوب هي احتمال ظهور عيب في التصميم ربما يكتشفه بعض متخصصي كسر الشفرة مما يؤدي (أو ربما أدى بالفعل فمن يدري؟!) إلى منح المتلصصين القدرة على اختراق الاتصالات الحساسة، ولكن حتى الآن لم يثبت أمر كهذا برغم الاختبارات المكثفة التي أُجريت على هذا الأسلوب، ولكن الأمر الذي يثير الشكوك هو أن وكالة الأمن القومي الأمريكية أوقفت في عام ١٩٩٦م دعمها لهذه الخوارزمية!! [Pfleeger 1997].

٢) عدد مرات تنفيذ العملية الرياضية

لماذا يتم تنفيذ العملية الرياضية ١٦ مرة؟ وهل هذا العدد كاف؟ لأن كل مرة يتم فيها تنفيذ العملية الرياضية تتبعثر معلومات النص الصريح في النص المشفر، وليس من الواضح أن ست عشرة دورة كافية لبعثرة المعلومات بالمستوى المطلوب. ولتوضيح ذلك فباستخدام دورة واحدة فإن كل رقم ثنائي من النص المشفر يتأثر فقط بعدد محدود من الأرقام الثنائية في

النص الصريح. وبتنفيذ العملية الرياضية عدداً أكبر من المرات تتم بعثرة هذه المعلومات بشكل أكبر بحيث لا يبقى أي رقم ثنائي في النص المشفر معتمدًا على عدد محدود من الأرقام الثنائية في النص الصريح.

وقد أظهرت التجارب التي أجرتها وكالة الأمن القومي الأمريكية وشركة "آي بي إم" أن تنفيذ العملية ثمان مرات فقط تكفي للتخلص من أي تبعية لحروف النص المشفر، وبذلك فتنفيذها ست عشرة مرة يجعلها آمنة بما فيه الكفاية.

٣) طول المفتاح

لعل هذه النقطة هي أهم النقاط التي أثيرت حول هذا الأسلوب للتشفير فقد كان طول المفتاح في خوارزمية "آي بي إم" السابقة (والتي مهدت الطريق لهذه الخوارزمية) هو (١٢٨) رقمًا ثنائيًا بينما يستخدم نظام (DES) مفتاحًا طوله (٥٦) رقمًا ثنائيًا فقط. وزيادة طول المفتاح تعني مجهوداً أكبر يتعين على من يحاول كسر الشفرة أن يبذله في محاولاته لإيجاد المفتاح.

٤-٤- كيفية كسر شفرة أسلوب (DES)

بمجرد عثور المتلصص على جزء من نص صريح وما يقابله من نص مشفر فهو سيحاول بالطبع التوصل إلى المفتاح الذي تم به التشفير، وذلك بفرض أن هذا المفتاح نفسه سوف يستخدم لتشفير نصوص أخرى. وبمعرفة المفتاح يمكن للمتلصص فك شفرة أي نص سبق تشفيره باستخدام هذا المفتاح بسهولة.

١) استراتيجية الهجوم:

استراتيجية الهجوم هي الأسلوب العشوائي، أي التجربة والخطأ، ويكون ذلك بتشفير النص الصريح المعروف باستخدام سلسلة من المفاتيح

واستمرار تجربة مفاتيح جديدة حتى يطابق النص المشفر الناتج نظيره المشفر الذي سبق الحصول عليه، وهناك عدد من المفاتيح المطلوب تجربتها قدره (٥٦٢) في المفتاح الذي يبلغ طوله (٥٦) رقمًا ثنائيًا. فإذا استطاع المتلصص تجربة مفتاح واحد كل ١٠٠ مللي ثانية ، فالوقت المطلوب لتجربة جميع المفاتيح سيكون (٧,٢ × ألف مليون مليون) ثانية أي حوالي ٢٢٨ مليون سنة! أما إذا استغرق الاختبار ١ مللي ثانية فقط فالوقت المطلوب لن يتجاوز ٢,٢٨٠,٠٠٠ سنة أي مليونا سنة فقط! حتى لو توصلت التقنية إلى زمن قدره "نانو ثانية" (جزء من ألف مليون جزء من الثانية) وهو أمر لا تستطيعه التقنيات الحالية في مستهل القرن الحادي والعشرين، فإن زمن البحث سيظل أكبر من عامين بفرض استمرار العمل على مدار الساعة دون حدوث أي فشل للأجهزة أو البرامج.

٢) المعالجة المتوازية:

من المنطقي أن يقودنا التفكير إلى تجربة "المعالجة المتوازية" باستخدام عدة معالجات تقوم كلها بمعالجة المشكلة آنيًا، فإن (الرقاقة Chip) الواحدة التي تستطيع معالجة مفتاح واحد كل "ميكروثانية" (جزء من مليون جزء من الثانية) تستطيع تجربة (٨٦ مليار) مفتاح في اليوم الواحد، أي أنها تحتاج إلى مليون يوم لتجربة جميع المفاتيح (حوالي ٧٠ ألف مليون مليون عملية). يعني ذلك باختصار أن مليون رقاقة تعمل على التوازي بهذا المعدل يمكنها تجربة جميع المفاتيح في يوم واحد، ومثل هذه الآلة لن يقل ثمنها عن ٥٠ مليون دولار!

٣) أسلوب هيلمان المقترح:

هناك وسيلة أخرى اقترحها "هيلمان" منذ فترة [Helman 80] ولكنها لم تنجح في ذلك الوقت لقصور تقنيات الحاسب آنذاك. وتتلخص هذه الطريقة

في إدخال جزء من النص الصريح لآلة التشفير (دون معرفة المفتاح المستعمل) للحصول على نص مشفر ، وبفرض إتاحة الوقت الكافي ومساحة التخزين الكافية فيمكن الحصول على كافة النصوص المشفرة الممكنة وعددها ($٢^{٥٦}$) باستخدام كافة الاحتمالات الممكنة للمفتاح، ويمكن بعد ذلك كشف المفتاح الذي استخدم في التشفير بفحص هذه النتائج، ووفقًا لمقترح "هيلمان" فهذا الحل يخفض عدد المحاولات إلى $٢^{٣٧}$ أو $١,٤ \times ١٠^{١١}$ محاولة، وباستخدام المعالجة المتوازية وبانخفاض أسعار المعالجات وازدياد سرعتها بعد مضي عشرين عامًا الآن من مقترح "هيلمان" يمكن إنتاج آلة تستطيع قهر هذا النوع من أساليب التشفير.

٤) شفرة اليابان الجديدة:

وآخر التطورات في هذا المجال هي إعلان اليابان مؤخرًا عن استخدامها لشفرة من هذا النوع تستخدم مفاتيح تشفير بطول ١٢٨ رقمًا ثنائيًا مما يجعل فرص كسر الشفرة التي تستخدم هذا الأسلوب تدخل في دائرة الاستحالة (على الأقل في الوقت الحاضر).

٥- التشفير باستخدام المفتاح العلني

٥-١- كيفية عمل النظام

التشفير باستخدام المفتاح العلني (أو غير المتماثل) تم اختراعه بواسطة "ديفل وهيلمان" في عام ١٩٧٦م ، وهو حل يجمع بين كونه عمليًا جدًا وكونه حل ذكي. ويقدم هذا الأسلوب فوائد لم تكن متاحة بواسطة أسلوب التشفير باستخدام المفتاح السري. وقد تم تصميم هذا الأسلوب ليناسب ثورة الاتصالات والعالم الذي بدأ يعيش عصر شبكات المعلومات، ولذلك فخوارزمية التشفير تكون معروفة للجميع، ويستطيع كل فرد في المجتمع أن يحتفظ بزوج خاص به من المفاتيح، أحد هذين المفتاحين سيكون "مفتاح

التشفير" وتكون قيمته معلنة، ومنشورة بواسطة وكالات خاصة تتولى نشر "دليل لمفاتيح التشفير المعلنة" (ويوجد حاليًا على شبكة الإنترنت أكثر من موقع يحتفظ بمفاتيح التشفير العلنية للعديد من الأشخاص، ويمكن الدخول إلى أحد هذه المواقع والاستعلام عن مفتاح التشفير العلني لأي شخص مطلوب مراسلته). أما المفتاح الثاني فهو مفتاح "فك الشفرة" والذي لا يكون معلومًا إلا للمتلقي وحده. وبذلك يمكن أن يكون لكل شخص (أ) في المجتمع دالة "تشفير" ت‌ا () معروفة للجميع، ودالة "فك شفرة" فا () لا تكون معلومة إلا للشخص (أ) وحده. ويتم تكوين كل زوج من المفاتيح بحيث تكون له الخاصية التالية:

لكل رسالة (ر) فإن فا (تا (ر)) = ر

أي بتطبيق مفتاح فك الشفرة "السري" على الرسالة التي تم تشفيرها بواسطة مفتاح التشفير "العلني" يمكن استعادة النص الأصلي للرسالة.

هذه الخاصية هي التي يعمل على أساسها المفتاحان السري والعلني. ومن البديهي أن نتأكد من عدم اعتماد أي من المفتاحين على الآخر، بمعنى أن معرفة مفتاح التشفير العلني لا تؤدي إلى معرفة مفتاح فك الشفرة السري.

مما يتميز به أسلوب التشفير باستخدام المفتاح العلني عن التشفير باستخدام المفتاح السري أن مرسل الرسالة يرسلها وهو مطمئن تمامًا لعدم إمكان تعديلها في الطريق (أو الصعوبة الكبيرة التي تكتنف هذه العملية)، كما أنه لا يحتاج إلى الاتفاق المسبق مع الشخص الذي يراسله على مفتاح سري لا يعلمه إلا كلاهما. بالإضافة إلى ذلك فلا توجد خشية من تسرب المفتاح أو الاضطرار إلى توزيعه على أشخاص كثيرين مثلما هو الحال مع أسلوب

المفتاح السري، ومن مزايا هذا الأسلوب كذلك إمكانية استخدام "التوقيعات الرقمية" والتي سنخصص لها القسم التالي.

٥-٢- التوقيعات الرقمية

يسمح استخدام التوقيع الرقمي لمتلقي الرسالة بالتأكد من شخصية المرسل والتأكد من أن محتويات الرسالة لم تخضع لأي تعديل خلال رحلتها. وذكر "رايت" أن (التوقيعات الرقمية تتيح للاتصالات الإلكترونية درجة من المخاطرة أقل من التوقيعات المخطوطة باليد التي اعتدنا عليها في الصور التقليدية للاتصالات المكتوبة) [Wright 1994].

ويعمل التوقيع الرقمي على النحو التالي:

بالإضافة إلى الخاصية: "فأ (تأ (ر)) = ر" فإنه يلزم أن يكون للمفتاحين العلني والسري كذلك الخاصية: "تأ (فأ (ر)) = ر" ، وبذلك يمكن إنتاج توقيعات رقمية موثوق بها.

إذا أراد شخص ما (أ) إرسال رسالة موقعة وموثقة إلى شخص آخر (ب) فإنهما يستطيعان تنفيذ ذلك على النحو التالي:

١) يعالج الطرف المرسل (أ) الرسالة المرسلة باستخدام مفتاح فك التشفير الخاص به [فأ (ر)].

٢) يعالج الطرف المرسل (أ) الرسالة بعد ذلك باستخدام مفتاح التشفير العلني للطرف المستقبل (ب) [تب (فأ (ر))].

٣) يتم إرسال الدالة الناتجة عن ذلك وهي تب (فأ (ر)) إلى الطرف المستقبل (ب).

٤) يقوم الطرف المستقبل (ب) باستخدام مفتاحه السري لفك التشفير فتنتج الدالة التالية: فب (تب (فأ (ر))) = فأ (ر).

٥) طالما أن الرسالة معروف أنها مرسلة من طرف المرسل (أ) فإن المتلقي (ب) يستطيع استخدام مفتاح (أ) العلني لمعالجة الدالة فا (ر) التي حصل عليها من أجل التوصل إلى الدالة تا (فا (ر)) والتي هي نفسها الرسالة الأصلية (ر) لأنه سبق القول أن تا (فا (ر)) = ر.

مادام الطرف (أ) وحده هو الذي يكون بمقدوره معرفة المفتاح المستخدم مسبقًا ليجعل الرسالة ذات معنى عند تشفيرها بواسطة مفتاح (أ) العلني فمعنى ذلك أن الرسالة هي بالفعل من طرف المرسل (أ) دون غيره (أليس هذا نوع من التوقيع).

٦- نظام (Rivest,Shamir & Adleman RSA) للتشفير

٦-١- فكرة النظام

برغم الفوائد الواضحة لأسلوب التشفير باستخدام المفتاح العلني فإنه لا يزال هناك تفاصيل هامة من قبيل كيفية بناء هذا الزوج من المفاتيح (التشفير/فك الشفرة). وأكثر الأساليب شيوعًا لتطبيق أسلوب التشفير باستخدام المفتاح العلني هو خوارزمية (RSA) التي تم تطويرها في عام ١٩٧٨م بواسطة العلماء الثلاثة "رايفست" و"شامير" و"أدلمان" وظلت حتى الآن شفرة مأمونة.

يعمل هذا النظام: "نظام RSA للتشفير باستخدام المفتاح العلني" (Rivest, Shamir & Adleman's public key encryption) عن طريق توليد مفتاحين من مفتاحٍ واحد: أولهما يستخدمه المرسل لتشفير الرسالة قبل إرسالها، والثاني يستخدمه المتلقي لفك شفرة الرسالة. وبالتالي فإن المتلقي الحقيقي هو الوحيد الذي يمكنه فك شفرة الرسالة، ويمكن الحصول على هذا النظام في صورة (رقاقة Chip) يتم تركيبها في الحاسب. ولكن برغم أنه

تتوفر الآن هذه الرقائق الخاصة التي تقوم بعمليات التشـــفير وفـــك الشـــفرة للرسائل الحساسة قبل وبعد نقلها باستخدام هذا الأسلوب، إلا أن هذه الرقـــائق ليست متاحةً أو مسموحًا بها في كل دول العالم لاعتبارات الأمـــن القومـــي للدول الكبرى.

٦-٢- أسلوب عمل النظام

مفتاح التشفير وفك الشفرة في هذا الأسلوب يعتمـــدان علـــى عـــرض الرسالة كرقم، على أن يتم رفع قوة (أس) هذا الرقم إلى قوة معينة ثم يتم أخذ الرقم الصحيح الناتج دون الإشارة (Modulus) أي أن مفتاح التشفير يصبح: ت|(ر) = $ر^{ت}$ |ن| ، ومفتاح فك الشفرة يصبح: ف|(ر) = $ر^{ف}$ |ن| .

وبذلك فكل مستخدم للنظام يحدد مجموعة مكونة من ثلاث قيم هـــي: "ت"، "ف" ، "ن" بحيث تحدد القيمتان "ت" و"ن" معًا مفتاح التشفير العلني، أما القيمتان "ف" و "ن" فتحددان معًا مفتاح فك الشفرة السري. ويتم اختيار الرقم "ن" كحاصل ضرب رقمين أولين كبيرين، كما يتم اختيار قيمـــة "ف" كرقـــم صحيح عشوائي ضخم، ويتم اختيار قيمة "ت" باشتقاقها من "ف". على هـــذا النحو يصبح النظام على مستوى عال من الأمن، فدرجة أمن النظام تتوقـــف على الصعوبة التي يواجهها المرء في محاولة التوصل إلى قيمـــة "ن" بعـــد حصوله على مفتاح التشفير العلني، وهو أمر سهل.

٧- أسلوب التشفير المودع (EES)

٧-١- نشأة النظام

أسلوب (التشـــفير المـــودع Escrowed Encryption System) أو (EES) هو نظام تشفير جديد يعتمد على المفتاح السري، وقد تـــم تطويـــره بواسطة الحكومة الأمريكية وقد شارك في تطويره كل من "ســـكيب جـــاك" و"كليبر" و"كابستون"، وهذان الأخيران قاما بإعداد رقاقة تحتوي على النظـــام

سُميت (رقاقة كابستون Capstone Chip) ورقاقة أخرى سُميت (رقاقة كليبر Clipper Chip) ، وكل من الرقاقتين تستخدمان خوارزمية (سكيب جاك Skipjack Algorithm) ، ومن شأن هذه الرقاقات أن تسهل استخدام هذا الأسلوب (EES) مع نظام كنظام الهاتف مثلاً لتشفير المكالمات الهاتفية. وعلى العكس من نظام (DES) فإن كل تفاصيل خوارزمية (EES) تعتبر من الأسرار الاستراتيجية للولايات المتحدة الأمريكية [Pfleeger 1997]. ومن ثم فتقييم هذا النظام لا يمكن أن يعتمد كسابقه على أسلوب التقييم العلني التقليدي، فنظام (DES) ثبت أمنه بعد تحليله بواسطة الخبراء وبعد ثبوت مقاومته لمجموعة من محاولات كسر الشفرة؛ بينما النقد الموجه لنظام (EES) استمد قوته من ظهور بعض المشاكل في بداية تصنيع الأجهزة التي تستخدمه [Clark 1994] ، وظهور المشاكل في هذا الوقت المبكر من مراحل الإنتاج يعتبر دليلاً على عدم نضج التصميم بشكل كاف.

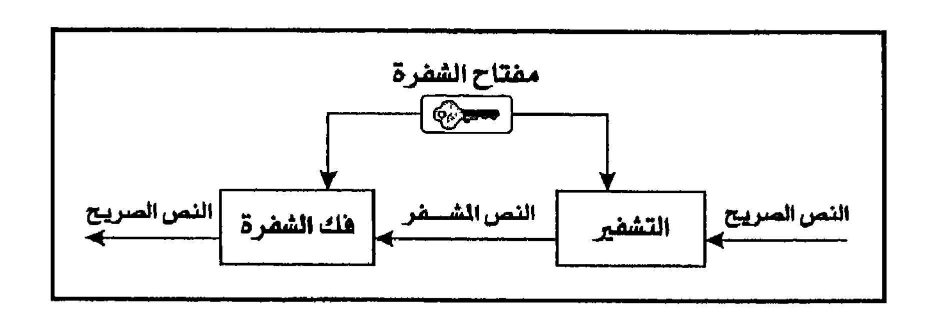
٧-٢- تشفير المكالمات الهاتفية

في عام ١٩٩٢م أعلنت شركة "إيه تي آند تي" (AT&T) عن إنتاج جهاز هاتف يسمح بتشفير الاتصالات الصوتية (وبالذات الهاتفية منها) [Denning 1993]. ويتم ذلك بتحويل المكالمة أولاً إلى إشارة رقمية (Digital) ثم تشفيرها ثم إعادة تحويل النص المشفر إلى إشارة تناظرية (Analog) لنقلها عبر شبكة الهاتف الصوتية ، ثم عكس هذا الإجراء لدى الطرف المستقبل لفك الشفرة. وكان في مقدور هذه الأجهزة توليد مفتاح شفرة جديد في كل محادثة وتشفير المفتاح نفسه ثم إرساله إلى الجهاز المستقبل قبل إجراء المحادثة المشفرة.

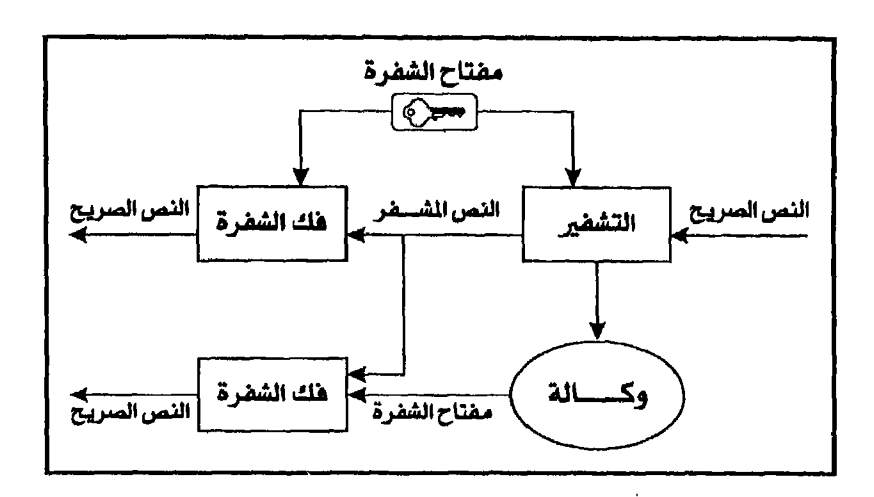
وقد سبب هذا المنتج عند ظهوره مشاكل كثيرة للجهات الأمنية وللشرطة مما منعها من متابعة العصابات الإجرامية، برغم حصولها على إذن من القضاء بالمتابعة والتنصت. ولذلك تم تعديل هذا المنتج فيما بعد،

بحيث تستطيع الأجهزة الأمنية أن تكسر هذا النوع من التشفير دون الحاجة إلى إضعافه فيتمكن الآخرون من كسره. وكان الدافع الرئيسي وراء إنتاج نظام (EES) هو ما ثار حول نظام (DES) من شكوك مع تطور العتاد وازدياد سرعة المعالجة، وما صاحب ذلك من انتشار واسع لأسلوب المفتاح العلني في التشفير (بالذات نظام RSA) مما جعل الجهات الأمنية تخشى من استخدام العصابات الدولية لنظام (RSA) مع مفاتيح صعبة الاختراق، ولذلك تم التوصل إلى نظام (EES) بحثاً عن أمرين: الأمر الأول هو الحصول على شفرة أقوى، والثاني هو تمكين الشرطة من كسر شفرة الرسائل المشفرة .[Bowyer 1996]

يبين الشكل (٩-٤) أسلوب التشفير التقليدي (المفتاح السري)، بينما يبين الشكل (٩-٥) أسلوب التشفير المودع (EES) ، وبمقارنة الشكلين يمكن اكتشاف الفرق بينهما.



الشكل (٩-٤) أسلوب التشفير التقليدي



الشكل (٩-٥) أسلوب التشفير المودع

يتم إيداع مفاتيح الشفرة لدى أي وكالة موثوق بــــها، ولحمايــــة أمــن التشفير يمكن تقسيم المفتاح إلى أجزاء بحيث يتم إيداع كل جزء لدى وكالــــة معينة. وعند صدور حكم من المحكمة بمراقبة محادثة معينــــة تــأتي هــذه الوكالات بأجزاء المفتاح التي لديها وتسلمها للشرطة التي تتولى إدخالها إلـــى جهاز فك التشفير حتى يمكن التنصت على المحادثة.

٧-٣- كيفية عمل النظام

عملية التشفير التي اخترعها "سكيب جاك" والتي يعمل على أساســـها نظام التشفير المودع هي عملية متكررة مثل تلك الخاصــــة بنظــام (DES) ولكنها تتكرر ٣٢ مرة (بدلاً من ١٦)، وتستخدم مفتاحًا من ٨٠ رقمًا ثنائيًـــا (بدلاً من ٥٦) وتقوم بتقسيم النص الصريح إلى وحدات كل منها مكون مــن ٦٤ رقمًا ثنائيًا.

يحمل كل جهاز (أو وحدة) تستخدم نظام (EES) عند إنتاجها رقمًا متسلسلاً طوله ٣٠ رقمًا ثنائيًا [Denning 1993] ولها مفتاح خاص بها، يُسمى (مفتاح الوحدة Unit Key)، مكون من ٨٠ رقمًا ثنائيًا ، وكل طراز من الأجهزة له مفتاح خاص مشترك بين وحدات الطراز (أو المجموعة) ويُسمى (مفتاح المجموعة Family Key) الذي تشترك فيه كل وحدات الطراز. ويبين الشكل (٩-٦) كيف يتم تشغيل وحدة (EES)، فكل وحدة يتم توليد مفتاحها من رقمها المتسلسل بطريقة غير مباشرة ويتم إيداع هذا المفتاح لدى وكالتين من (وكالات الإيداع Escrow Agents)، وهذه الوكالات في الولايات المتحدة تكون إحداها أحد مكاتب المعهد القومي الأمريكي للمواصفات والتكنولوجيا والأخرى أحد مكاتب وزارة الخزانة الأمريكية. ويتم إيداع مفاتيح الشفرة عن طريق الخطوات التالية التي أظهرناها على الشكل (٩-٦):

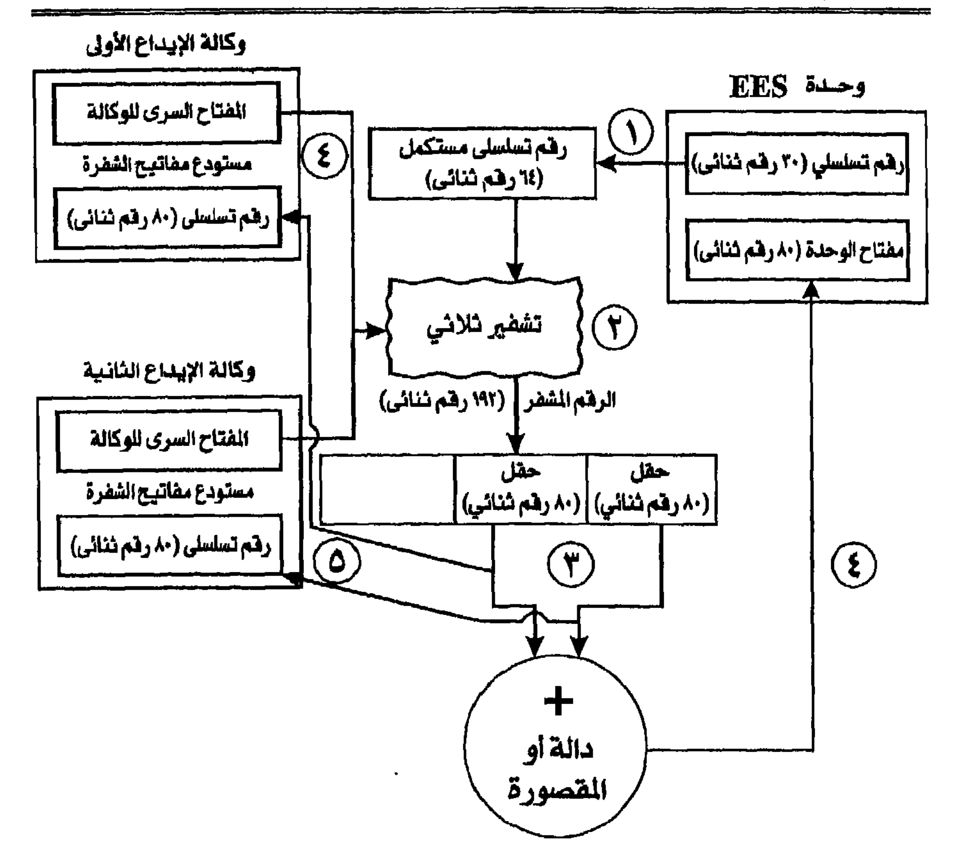
١) يتم استكمال الرقم التسلسلي للوحدة (٣٠ رقمًا ثنائيًا) بعدد إضافي من الأرقام الثنائية لملء الوحدة المكونة من ٦٤ رقمًا ثنائيًا (وهي وحدة التشفير في نظام EES).

٢) يتم بعد ذلك تشفير هذه الوحدة (التي تمثل الرقم التسلسلي) ثلاث مرات باستخدام مفتاح التشفير السري لكل من الوكالة الأولى والوكالة الثانية معًا. يؤدي ذلك إلى الحصول ـ من مرات التشفير الثلاث ـ على ثلاث قيم (كل منها مكون من ٦٤ رقمًا ثنائيًا) يتم ضمها معًا لتكوين رقم واحد مشفر (مكون من ١٩٢ رقمًا ثنائيًا).

٣) الأرقام الثنائية الثمانون الأولى تصبح هي النصف الأول من مفتاح الوحدة (المودع لدى الوكالة الأولى)، بينما تصبح الأرقام الثمانون التالية النصف الثاني من مفتاح الوحدة (المودع لدى الوكالة الثانية). وتسجل كل وكالة إيداع لديها، في مستودع لمفاتيح الشفرة، كلاً من الرقم التسلسلي للوحدة ونصف مفتاح الوحدة المودع لديها.

٤) يتم بعد ذلك توليد مفتاح الوحدة بتطبيق دالة (أو المقصورة Exclusive OR) على نصفي المفتاح (الأرقام الثنائية الثمانون الأولى والثانية) المودعين لدى وكالتي الإيداع. وبذلك تكون الوكالتان مشاركتين في توليد مفتاح الوحدة لكل جهاز (EES) لأن كلاً منهما تستخدم مفتاحها السري في توليد مفتاح الوحدة. ولكن كل وكالة لا تعرف مفتاح الوحدة بالكامل، وبذلك فإن أي محاولة بحث عشوائي عن مفتاح الوحدة تتطلب البحث في مدى هائل من القيم الممكنة للمفاتيح ($٢^{٨٠}$ احتمال)، ولكن مفتاح الوحدة يمكن معرفته بسهولة باشتراك الوكالتين معًا.

٥) تحتفظ كل من الوكالتين بنصف مفتاح التشفير المودع لديها في مستودع مفاتيح الشفرة، وعند الحاجة إلى المفتاح يمكن إعادة تركيبه بإخضاع النصفين لدالة (أو المقصورة Exclusive OR).



شكل (٩-٦) كيفية عمل نظام التشفير المودع (EES)

٧-٤- مفتاح الجلسة السري

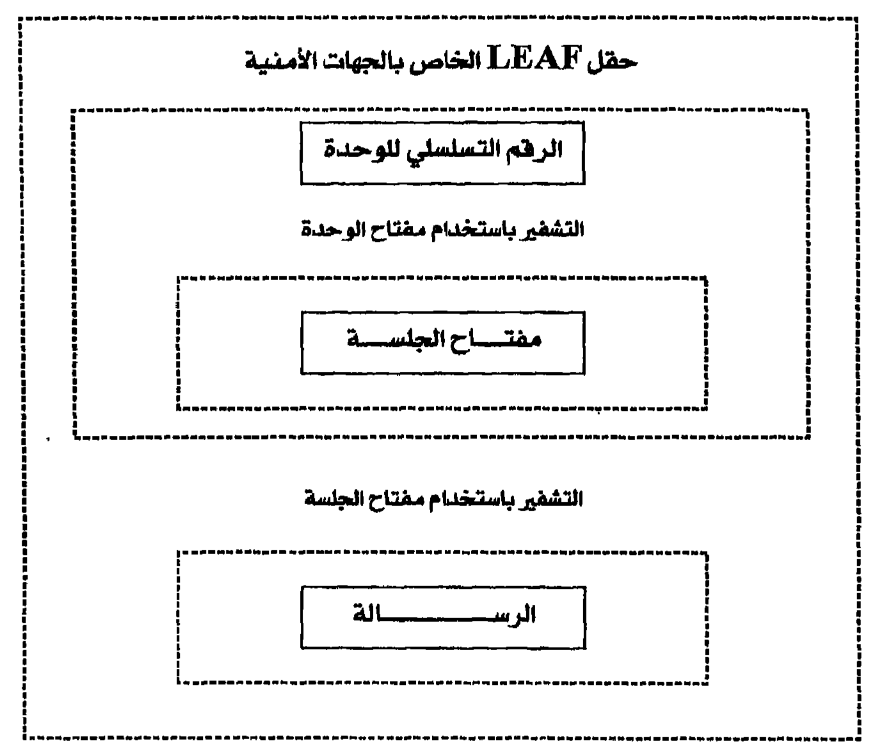
عندما ترغب وحدتان (EES) في تنفيذ اتصال مأمون بينهما تتفق الوحدتان على (مفتاح جلسة Session Key) مخصص لهذه المحادثة بالذات،

ويستخدم هذا المفتاح لتوليد مقاطع من المعلومات المشفرة طول كل منها ٦٤ رقمًا ثنائيًا، ويتم تبادل هذه المقاطع المشفرة بين الوحدتين، والوسيلة التي يتم الاتفاق بها على مفتاح الجلسة غير معلن عنها من قبل الحكومة الأمريكية. ولو أن "ديفل" و"هيلمان" قد اقترحا منذ فترة طويلة وسيلة جيدة وبسيطة للاتفاق على "مفتاح الجلسة السري" [Diffle 1976] ويعتقد كثير من المتخصصين أن هذه الوسيلة المقترحة هي الوسيلة المستخدمة حاليًا في الاتفاق على مفتاح الجلسة في نظام التشفير المودع [Bowyer 1996].

وتعتمد هذه الوسيلة على أن يكون هناك رقم متفق عليه بين الطرفين، ثم يقوم الطرفان (المرسل والمستقبل) برفع هذا الرقم إلى قوة مختارة عشوائيًا (أس عشوائي) ثم يتبادل الطرفان هذه القيمة، وبعد ذلك يرفع كل منهما القيمة التي حصل عليها من الطرف الآخر عن طريق هذا التبادل إلى نفس الأس العشوائي الذي اختاره من قبل، وبذلك يصبح لدى كل من الطرفين مفتاح مشترك.

٧-٥- كيفية تشفير أجزاء الرسالة

يبين الشكل (٩-٧) كيفية تشفير أجزاء رسالة (EES)، فكل رسالة متبادلة بين الطرفين تكون مكونة من أجزاء منفصلة: الجزء الأول هو الرسالة نفسها والتي يتم تشفيرها باستخدام "مفتاح الجلسة"، والجزء الثاني هو مفتاح الجلسة نفسه والذي يتم تشفيره باستخدام مفتاح الوحدة، أما الجزء الثالث فهو رقم الوحدة التسلسلي. الجزءان الثاني والثالث يتم تشفيرهما باستخدام "مفتاح المجموعة". مفتاح الجلسة المشفر (الجزء الثاني) ومفتاح الوحدة التسلسلي (الجزء الثالث) يتم الاحتفاظ بهما في حقل معين يرمز له باسم (الحقل الخاص بالجهات الأمنية Law-Enforcement Access Field) أو (LEAF).



شكل (٩-٧) كيفية تشفير أجزاء رسالة (EES)

٧-٦- كيفية فك شفرة الرسالة بواسطة الشرطة.

لو أن الشرطة سُمح لها بحق التنصت على اتصال تم تشفيره باستخدام أسلوب التشفير المودع فإنها تستطيع استخدام مفتاح المجموعة لفك شفرة هذا الحقل (LEAF) مما يمنحها إمكانية التوصل إلى الرقـم التسلسـلي للوحـدة ومفتاح الجلسة الذي تم تشفيره بواسطة مفتاح الوحدة. وهنا تحمل الشـرطة الرقم التسلسلي للوحدة وتصريح التنصت إلى وكالتي الإيداع فتقوم كل وكالة باستخراج نصف مفتاح الوحدة المودع لديها من مسـتودع مفـاتيح الشـفرة

الخاص بالوكالة. وبذلك تستطيع الشرطة استعادة مفتاح الوحدة من وكـــالتي الإيداع واستخدامه لفك شفرة مفتاح الجلسة (الذي ذكرنا أنه قد تـــم تشـــفيره باستخدام مفتاح الوحدة)، وعندئذ وبمجرد حصول الشرطة على مفتاح الجلسة تستطيع فك شفرة الرسالة.

يتضح من ذلك أن معرفة محتويات حقل (LEAF) تتيح فـــي النهايـــة التوصل إلى فك الشفرة، ويعني ذلك أن هذا الحقل يعتبر نوعًا من فـــيروس (باب المصيدة Trapdoor) (الذي يُمكّن من كسر شفرة الاتصالات المؤمنـــة بواسطة نظام (EES).

٧-٧- تقييم أسلوب التشفير المودع

شكلت الحكومة الأمريكية في عام ١٩٩٢م لجنة سُميت "لجنة بريفـــل" لفحص أسلوب التشفير المودع وتقييمه، وفي عام ١٩٩٣م توصلت هذه اللجنة إلى النتائج الإيجابية التالية [Pfleeger 1997]:

١) بفرض أن تكلفة قوة المعالجة في الحاسبات تنخفض إلى النصف كل ثمانية عشر شهرًا فسوف تنقضي ٣٦ عامًا قبل أن تصل تكلفة كسر خوارزمية "سكيب جاك" بأسلوب البحث المكثف لتتساوى مع التكلفـــة الحالية لكسر أسلوب(DES) ، ولذلك فليس هناك خشية مـــن كســـر خوارزمية "سكيب جاك" خلال الثلاثين أو الأربعين سنة التالية.

٢) لا يوجد احتمال يذكر بإمكان كسر هذه الخوارزمية من خلال أسلوب بحث مختصر آخر.

٣) برغم أن التركيب الداخلي لخوارزمية "سكيب جاك" يجب أن يظـــل سرًا من أجل أغراض حمايـــة الأمـــن القومـــي إلا أن قـــوة هـــذه الخوارزمية في مواجهة خبراء كسر الشفرة لا تعتمد على سرية هـــذه الخوارزمية.

الفصل العاشر

نظم أمن البيانات

موضوعات الفصل:

(١) دور نظم أمن البيانات.
(٢) الإمكانيات المتاحة في نظم التشغيل لتأمين البيانات.
(٣) الموارد التي يجب حمايتها.
(٤) مستويات الصلاحية لاستخدام البيانات.
(٥) التقارير التي تنتجها نظم أمن البيانات.
(٦) بعض نظم أمن البيانات المتوفرة بالأسواق.
(٧) المفاضلة بين نظم أمن البيانات.
(٨) أسلوب النسخ الاحتياطي ومعدلاته.
(٩) استعادة البيانات المفقودة.
(١٠) مستويات الأمن في مراكز الحاسب.


Converted by Tiff Combine - (no stamps are applied by registered version)

نتحدث في هذا الفصل عن النظم التي تكفل الأمن للبيانات، فنبدأ بتحديد دور هذه النظم وما هو مطلوب منها، ثم نتحدث عن الإمكانيات المتاحة في نظم التشغيل لتأمين البيانات، وخصائص نظام التشغيل المؤمَّن وقدراته. ثم نصنف الموارد التي يجب حمايتها في النظام، كما نتناول مستويات الصلاحية ومستويات الحماية.

نبين بعد ذلك أنواع التقارير التي تنتجها نظم أمن البيانات ومعدلات إخراجها. ثم ننتقل إلى عرض بعض نظم أمن البيانات الموجودة بالأسواق سواء لنظم الحاسبات المركزية أو الشخصية أو الشبكات المحلية. ونخصص قسمًا من هذا الفصل لتوضيح أسس المفاضلة بين نظم أمن البيانات لاختيار المناسب منها.

ننتقل بعد ذلك إلى موضوع النسخ الاحتياطي فنتحدث عنه كركن أساسي من أركان أمن البيانات، ثم نتحدث عن معدلات إنتاج النسخ الاحتياطية والوسائط التي تستخدم في حفظها، كما نبين كيفية استعادة البيانات المفقودة من النسخة الاحتياطية.

ونختتم هذا الفصل بموضوع هام أتمنى أن يأخذ حقه من التطبيق في عالمنا العربي وهو تصنيف مراكز الحاسبات من حيث مستوى الأمن فيها.

١-دور نظم أمن البيانات

١-١-مفهوم أمن البيانات

عندما نتكلم عن أمن البيانات (أو المعلومات إذا شئنا أن نكون أكثر دقة) فإننا نعني المحافظة على هذه المعلومات من الضياع أو التلف أو التغيير أو التسرب لغير المختصين، كما نعني المحافظة عليها من الأخطار الطبيعية كالحريق والزلازل والغرق بالمياه، ونعني كذلك المحافظة عليها من

الأخطار غير المقصودة مثل: الانقطاع المفاجئ للكهرباء أو للاتصالات في الشبكة، وأخيرًا نعني حمايتها من الأخطار المتعمدة مثل : الهجمات الإرهابية أو القنابل الموقوتة أو التزوير أو الاقتحام غير المشروع (Hacking) أو السرقة .... أي يمكن تعريف أمن البيانات باختصار على الوجه التالي:

"أمن البيانات هو تأمين وصول البيانات المطلوبة دون زيادة أو نقصان وفي الصورة السليمة الصحيحة إلى المستفيد المعني بها دون غيره في الوقت الملائم دون تأخير".

والمهم في مسألة الأمن ـ كما ذكرنا من قبل ـ ليس أن نضع الإجراءات المحكمة، وإنما المهم أن تكون إجراءاتنا عملية وميسرة. فمن السهل على أي شخص أن يبني قلعة مسلحة محكمة التحصينات ولكن من الصعب أن يجعل الإقامة في هذه القلعة سهلة وممكنة وممتعة لسكانها.

ومع الانتشار المتزايد (والمخيف) لشبكات المعلومات لتطوي المسافات بين الدول ولتشمل العالم كله جاعلة منه قرية صغيرة، مع هذا الانتشار ازدادت أهمية قضية الأمن ، وأصبحت هذه القضية تهم رجل الأعمال والمدير وكل من لديه معلومات، وأصبحت تهم المستفيد العادي والشركات التي تقدم خدمات المعلومات ومصممي النظم والتطبيقات، وكذلك الشركات المطورة للأجهزة والبرمجيات، بل هي تهم رجال القانون والتشريع ومتخصصي الاتصالات والمدرسين والطلاب ومسئولي الرقابة؛ سواء المالية أو الإدارية، بل هي مهمة كذلك للصحفيين. وعلى رأس هؤلاء جميعًا مسئولو أمن المعلومات. أي إنها باختصار تهمنا جميعًا، وهذا هو ما أعطى نظم أمن البيانات أهمية قصوى في عالم اليوم.

١-٢ المطلوب من نظم أمن البيانات

يجب أن توفر نظم أمن البيانات ثلاثة متطلبات أساسية ومهمة [Pfleeger 1997] هي:

١) **خصوصية البيانات (Data Confidentiality):**
بحيث لا يتمكن المتطفلون من الوصول إلى البيانات.

٢) **سلامة البيانات وتكاملها (Data Integrity):**
بحيث لا تتعرض البيانات لأي تبديل أو تغيير بوسيلة غير مشروعة.

٣) **إتاحة البيانات (Data Availability):**
بحيث تتوافر البيانات المطلوبة للمستفيد عند طلبها.

ويطلق على هذه المتطلبات الثلاثة أحيانًا الاختصار (CIA)، لما لهذا الاختصار من دلالة.

ولكي تستطيع هذه النظم تحقيق هذه المتطلبات الأساسية من أجل حماية البيانات وتأمينها يجب أن تتوفر فيها هذه العوامل الأساسية:

١) أن يكون النظام شاملاً أي يتطرق إلى جميع المراحل التي تمر بها البيانات وكذلك جميع الأحوال التي تكون عليها البيانات.

٢) أن يكون كاملاً بمعنى ألا تكون به ثغرات يمكن الاختراق من خلالها.

٣) أن يكون غير مرئي للإنسان بقدر الإمكان حتى تقل فرص اختراقه.

٤) أن يصعب تتبعه وفك رموزه أو فهم كيفية تركيبه لغير المختصين، كما يجب أن يكون من الصعب تعطيله أو إيقافه عن العمل.

٥) أن يكون موثقًا.

٦) أن يتم اختباره جيدًا بحيث تكون درجة الثقة به أقرب ما يكون إلى ١٠٠% فاستخدام نظام حماية غير موثوق به أخطر كثيرًا من عدم استخدام نظام حماية على الإطلاق.

٧) ألا تكون له أعباء كثيرة (Overheads) على نظام التشغيل أو نظم التطبيقات.

٨) سهولة ومرونة منح الصلاحيات وإلغائها.

٩) سهولة ومرونة ودقة تحديد شخصية المستفيد وتحديد صلاحياته.

٢- الإمكانيات المتاحة في نظم التشغيل لتأمين البيانات

يقوم العديد من نظم تشغيل الحاسبات بتوفير أساليب عديدة لتأمين البيانات والبرمجيات، وتزداد أهمية دور نظام التشغيل في تأمين البيانات كلما ازداد عدد المستخدمين للنظام، وكلما بعدت المسافة بين الطرفيات التي تستخدم النظام وبين وحدة المعالجة المركزية، فعلى نظام التشغيل أن يحمي النظام ككل من المستفيدين وأن يحمي المستفيدين أنفسهم من بعضهم البعض. فكيف نعرف إذا ما كان نظام التشغيل مؤمنًا أم غير مؤمن؟ لابد لنا من أن نحدد: خصائص نظام التشغيل المؤمَّن (Properties)، ووظائف التأمين في نظام التشغيل (Functions)، وقدرات نظام التشغيل الآمن (Capabilities) وذلك من أجل تحقيق أمن الحاسب ككل.

٢-١ خصائص نظام التشغيل المؤمَّن

يمكن تلخيص خصائص نظام التشغيل المؤمَّن في **قابليته للتحكم (Controllability) وتحقيقه للسلامة والأمن (Integrity) وقابليته للفحص (Auditability)** ، وهكذا نجد أنفسنا مرة أخرى أمام الاختصار (CIA). وهذه الخصائص الثلاث يعتمد بعضها على بعض بشكل كبير.

١) **القابلية للتحكم (Controllability):**

المقصود بها تلك الخاصية في النظام التي تجعله يسمح لمدير النظام

بالتحكم الكامل في الصلاحيات، مما يعطي الإدارة القدرة على التحكم فيمن يحق له من المستفيدين استخدام النظام وأي الموارد يستطيع هذا المستفيد الوصول إليها واستخدامها وبأي مقدار.

٢) السلامة والتكامل (Integrity):

يحقق نظام التشغيل خاصية السلامة عندما يثبت قدرته على حماية نفسه من المستفيدين الذين يستخدمونه، وعندما يستطيع فرض استخدام القواعد والسياسات الأساسية، وعندما يحمي المستفيدين وبياناتهم من بعضهم البعض.

في بعض الأحيان تعتمد خاصية السلامة في نظام التشغيل على بعض خصائص جهاز الحاسب نفسه (H/W) مثل تعدد حالات الأفضلية وآليات حماية الذاكرة، ولكنها في جميع الأحوال تعتمد على درجة الاطمئنان إلى التحكم الكامل (Content control) أي مدى تأكد مديري النظام من أن نظام التشغيل الذي يعتمدون عليه هو نفسه النظام المستخدم. ولكي يكون ذلك ممكنًا يجب أن يتحتم على الشخص الذي يريد إعادة تشغيل النظام أن يصل إلى أجهزة معينة لها حماية خاصة (مثل طرفية الكونسول أو خادم الملفات) أو أن يكون هذا الشخص من المستخدمين ذوي الأولوية أو أن يكون ذا صلاحيات خاصة تمكنه من تغيير بارامترات النظام، أي باختصار يفترض أن صلاحيات مديري النظام ومشغليه لابد أن تكون مختلفة عن صلاحيات المستخدم العادي.

٣) القابلية للفحص والمراجعة (Auditability):

هي الخاصية التي تمكن من فحص ومراجعة النظام ومواءمته، وفيما يختص بالأمن فإن نظام التشغيل الذي يمتاز بهذه الخاصية لابد أن يخرج التقارير التي تلفت انتباه الإدارة إلى أي سلوك غير عادي أو غير منتظر،

فلابد من إخضاع النظام بالكامل للمراقبة والمتابعة للتأكد من أدائه للوظائف المطلوبة منه ، وعلى مسئول أمن المعلومات بالمؤسسة أن يستخدم التقارير المستخرجة من النظام لتصحيح ما يلزم ، على أن يتم ذلك بصفة مستمرة.

٢-٢ وظائف التأمين في نظام التشغيل

تتضمن نظم التشغيل الآمنة في العادة الوظائف التالية والتي قد تكون في كثير من الأحيان مندمجة مع بعضها:

١) تمييز المستفيد (Identification):

لابد أن يكون لدى نظام التشغيل الآمن القدرة على التعرف على المستفيدين الذين يستخدمون الإجراءات والموارد، إما عن طريق اسم المستفيد وإما عن طريق رقم خاص به، وأبرز مثال على ذلك هو استخدام مميز المستفيد (User ID).

٢) التأكد من شخصية المستفيد (User Authentication):

لنظم التشغيل الآمنة القدرة على جمع الدلائل التي تؤكد شخصية المستفيد، وتأخذ هذه الدلائل عادة شكل أكثر من معلومة لا يعلمها إلا هذا المستفيد (مثل كلمة المرور)، أو أشياء لا تكون إلا في حوزته دون غيره (مثل المفاتيح أو بطاقة التعريف الممغنطة) ، أو دلائل تميز هذا المستفيد عن غيره (مثل بصمة الإصبع أو صورة قاع العين)، أو أفعال معينة لا يستطيع سوى هذا المستفيد أداءها (مثل بصمة الصوت أو التوقيع).

٣) ضوابط استخدام البيانات (Access control):

تستطيع نظم التشغيل فرض قواعد تحدد ماذا يستطيع كل مستفيد أن يصل إليه من موارد، وهذه القواعد تكون عادة نسبية أو متروكة لتقدير المستفيدين الذين يمتلكون البيانات أنفسهم، ويجب أن تكون هذه القواعد

واجية الاتباع، ويشرف على تنفيذ ذلك مسئول الأمن أو مدير النظام. ويعتبر نظام التشغيل آمنا إذا كان قادرا على فرض قواعد واضحة لاستخدام البيانات لا يمكن الحياد عنها أو الالتفاف حولها من جانب أحد من المستفيدين.

٤) إدارة ضوابط استخدام البيانات (Administration):

المقصود بها مجموعة الوظائف التي تمكن مسئول الأمن من إنشاء وصيانة المعلومات التي تتضمنها ضوابط استخدام البيانات ، أي القواعد التي تحكم استخدامها، مثل: السماح لمستفيد معين باستخدام مورد معين لفترة معينة، أو نزع هذه الصلاحية منه.

٥) تسجيل الوقائع (Logging):

تقوم معظم نظم التشغيل التي تتوخى الأمن بتسجيل وقائع استخدام البيانات مثل: حالات فشل الدخول إلى النظام، وحالات الخطأ في إدخال كلمة المرور، وتكرار محاولات الدخول الخاطئة إلى النظام من مستفيد معين، وهكذا.

٦) إخراج التقارير (Reporting):

يقوم الكثير من نظم التشغيل الآمنة بتحليل وترتيب البيانات التي يتم تسجيلها عن الوقائع الأمنية وإخراجها في شكل تقارير واضحة تسهل فهم الوقائع والربط بينها وتساعد بذلك على التصرف بشأنها بالشكل الصحيح.

٧) الإنذار (Alarms):

تصدر معظم نظم التشغيل الآمنة إنذارات (كأن تكون في صورة رسائل تعرض على وحدة "الكونسول" مثلاً) لتنبه مسئول النظام إلى الحالات التي تحتاج إلى التدخل السريع أو إلى اتخاذ إجراءات لتصحيح الوضع.

٨) الرسائل (Messages):

بعض النظم تصدر رسائل إلى المستفيدين من مالكي البيانـــات وإلـــى المسئولين عن إدارة موارد معينة (مثل الأقراص الممغنطة) عن اســتخدامات هذه البيانات أو الموارد وأي تعديل قد يطرأ عليها.

٢-٣- قدرات نظام التشغيل الآمن (Capabilities)

يشمل مفهوم الأمن في نظم التشغيل قدرة هذه النظـــم علـــى العـــزل (Isolation)، وتحقيق التوازن (Mediation):

١) العزل (Isolation):

تقوم نظم التشغيل الآمنة والتي يتعدد فيها المستفيدون بتحقيق نوع من العزل بين العمليات، كأن تقوم بالعزل بين برامج النظام وبرامج التطبيقـــات، أو بالعزل بين التطبيقات وبعضها، أو العزل بين المستفيدين وبعضـــــهم، أو العزل بين الأعمال (Jobs) وبعضـــــها أو العـــزل بيـــن المـــهام (Tasks) وبعضها، وكذلك العزل بين الأجزاء المختلفة في الذاكرة الافتراضية. ومـــن أمثلة هذا العزل استخدام نسخ مختلفة من نظام الاتصال المباشـــــر (CICS) مثلاً ، أو قدرة نظام التشغيل على منع كل مستفيد أو برنامج من التدخل فـــي مجال العنونة (Address space) الخاص بالمستخدم الآخر، وذلك في نظـــام التشغيل (MVS) على سبيل المثال، باستخدام مفتاح (Key) لكـــل مســتفيد خلال تنفيذ أعماله داخل الحاسب على أن يتولى نظام التشغيل بنفسه توليـــد هذا المفتاح دون أن يشعر به المستفيد. وأسلوب العزل هذا يمنع كل مســتفيد من التدخل في أعمال المستفيدين الآخرين أو التأثير عليها بأي شكل.

٢) تحقيق التوازن (Mediation):

تقوم نظم التشغيل الآمنة التي يتعدد فيها المستفيدون بتحقيق التشـــارك

في الموارد بين المستفيدين بشكل متوازن، وذلك عن طريق توزيع موارد النظام بأسلوب معين، حيث تفرض هذه النظم على مستخدمي البيانات ضرورة التشارك في الموارد. ويتم ذلك في نظم تشغيل الشبكات بالمرور الدوري على وحدات الشبكة لمعرفة حاجتها للعمل وهو ما يطلق عليه أسلوب "توكن" (Token) ، كما يتم توزيع موارد الحاسب على المستفيدين في نظم تشغيل الحاسبات الكبيرة عن طريق برنامج خاص يسمى "مدير الموارد" (Resource Manager) والذي يسمح بتشارك المستفيدين في الموارد. وفي معظم نظم قواعد البيانات يوجد نظام للإغلاق (Locking) لتنظيم استخدام المستفيدين للموارد ولاكتشاف وجود حالات "التوقف الدائم" (Dead Lock)، أو استحواذ لأحد المستفيدين على موارد الحاسب والعمل على حل هذه المشكلات.

وقد يتعارض في بعض الأحيان مفهوم العزل مع مفهوم التشارك، ولذلك يفضل أن يقوم نفس النظام بهاتين المهمتين حتى لا يحدث تعارض ويتحقق التوازن المطلوب.

٣- الموارد التي يجب حمايتها

٣-١- دخول المستفيد إلى النظام

لابد لكل نظام أمني أن يقوم بما يلي:

١) تمييز المستفيد عند دخوله إلى النظام، ويكون ذلك إما باستخدام رمز المستفيد (Userid) وهو الأسلوب الشائع أو استخدام أية وسيلة أخرى، ثم التحقق من شخصية المستفيد، ويتم ذلك عادة عن طريق كلمة المرور.

٢) بعد التحقق من شخصية المستفيد يجب تنظيم استخدام هـذا المستفيد لموارد النظام بمعنى السماح له باستخدام الموارد التي يحق له استخدامها على النحو المسموح له استخدامه (قراءة فقط / تعديل / حذف ...) وفي الوقت المسموح له بذلك ومن خلال الطرفية المحدد له استخدامها.

٣-٢- وصول المستفيد إلى الموارد

يسمح النظام الأمني للمستفيد باستخدام المورد إذا توفرت في المستفيد طالب الخدمة أحد الشروط التالية:

١) إذا كان المستفيد هو صاحب المورد (Owner) فيسمح له باستخدام الملفات الخاصة به على سبيل المثال.

٢) إذا كان رقم المستفيد وارداً ضمن القائمة التي تتضمن المسموح لهم باستخدام المورد وأن تحدد القائمة لهذا المستفيد صلاحية تتفق مع (أو تزيد على) الصلاحية التي يطلبها.

٣) إذا كانت المجموعة التي ينتمي إليها المستفيد تقع ضمن القائمة التي تتضمن المسموح لهم باستخدام المورد مع الصلاحية الكافية.

٣-٣- الموارد التي يتم تأمينها

لما كان الهدف من أي نظام أمني هو حماية الموارد وتأمينها، فما هي هذه الموارد التي يتعين على النظام الأمني أن يقوم بحمايتها ومراقبة استخدامها وتأمينها ضد سوء الاستخدام بكافة صوره وأشكاله؟

هذه الموارد هي ملفات البيانات سـواء الموجـودة علـى الأقـراص الممغنطة أو على الأشرطة الممغنطة والمسـاحات الخاصـة بالمسـتفيدين أنفسهم، مثل: (Datasets) في نظام التشغيل (MVS)، أو (Minidisks) فـي نظام التشغيل (VM)، هذا بالإضافة إلى كل ما يطلق عليه (الموارد العامـة General resources) مثـل: "الطرفيـات" والمعـاملات (Transactions) الموضوعة تحت حماية النظام لأهميتها ، سواء تلك المعاملات التي تتبع نظم إدارة قواعد البيانات مثل (IMS)، أو تلك التي تتبع نظم الاتصال المباشـر مثل (CICS)، هذا بالإضافة إلى البرامج التي يتم تنفيذها، والتطبيقات المهمة الخاصة بالمؤسسة، والإجراءات (Procedures)، إلـى جـانب الأقـراص الممغنطة والأشرطة الممغنطة.

ويمكن حصر الموارد العامة في الحاسبات الكبيرة والتي يمكن تأمينـها بواسطة النظام الأمني فيما يلي:

١) الأقراص الممغنطة.

٢) الأشرطة الممغنطة.

٣) الطرفيات.

٤) الطابعات.

٥) مساحات معينة من الذاكرة.

٦) الملفات وقواعد البيانات.

٧) المساحات الخاصة بالمستفيدين على الأقراص.

٨) البرامج.

٩) الإجراءات.

١٠) معاملات نظم قواعد البيانات.

١١) معاملات نظم الاتصال المباشر.

١٢) أوامر نظام التشغيل.

١٣) الشبكات.

١٤) أي موارد أخرى تهم المؤسسة ويتم تعريفها للنظام الأمني.

٤- مستويات الصلاحية لاستخدام البيانات

٤-١- الصلاحية العامة للموارد

يمكن تحديد مستوى عام للصلاحية (Universal Access Authority) لكل مورد ويسمح للكافة بهذا المستوى العام الذي قد يكون أحد المستويات التالية:

١) التحكم الكامل:

حيث يُسمح للمستفيد بصلاحيات كاملة على المورد تصل إلى حد إيقاف المورد عن العمل أو حتى حذفه (بالنسبة للملفات).

٢) التعديل:

حيث يُسمح للمستفيد باستخدام المورد لأغراض القراءة والكتابة معًا.

٣) القراءة:

حيث يُسمح للمستفيد باستخدام المورد لأغراض القراءة فقط دون غيرها.

٤) **التنفيذ:**

وهي صلاحية تقتصر على نظـام التشـغيل (MVS) حيـث يُسـمح للمستفيد بتنفيذ برامج معينة، ولكن لا يُسـمح لـه بـالاطلاع علـى محتويات هذه البرامج (Source code) أو نسخها.

٥) **بدون:**

حجب الصلاحية بالكامل عن المستفيد فلا يستطيع استخدام هذا المورد بأية صورة كانت.

٤-٢- مستويات الحماية

تتراوح مستويات حماية الموارد بين المنع الكامل والمنح الكامل علـى النحو التالي:

١) المنح الكامل أو الحجب الكامل للصلاحية عن بعض المستفيدين مـع تسجيل وقائع استخدام المستفيد للمورد باستمرار.

٢) السماح للمستفيد باستخدام أحد الموارد المحظور استخدامها على هـذا المستفيد لفترة محددة فقط إذا حاول استخدامها، مـع إرسـال رسـالة تحذير لصاحب المورد ليتصرف وفقًا للموقف إمـا بإيقـاف السـماح للمستفيد أو برفع الحظر عن المورد.

٣) حجب الصلاحيات تمامًا عن بعـض المـوارد وتسـجيل كـل مـن المحاولات الناجحة وغير الناجحة لاستخدام هذه الموارد.

٥- التقارير التي تنتجها نظم أمن البيانات

٥-١- متى يخرج النظام التقارير؟

لابد لكل نظام أمني أن يقوم بما يلي:

١) بعد قيام المستفيد بتنفيذ أي عملية يجب تسجيل هذه العملية في سجلات النظام الأمني مع كافة ملابساتها مثل: الوقت الذي تمت فيه والطرفية التي استخدمت في تنفيذها. وتستخدم هذه السجلات فيما بعد لاستخراج التقارير.

٢) إخراج تقارير دورية (أو حسب الطلب) لجذب انتباه الإدارة لأنشطة المستفيدين سواء الأنشطة العادية أو الأنشطة التي تقع في دائرة المخالفة، كما تظهر هذه التقارير أي انحراف عن الاستخدام المتوقع لموارد النظام.

إن تسجيل وقائع استخدام البيانات وإخراج التقارير المبوبة عن ذلك يساعد المؤسسة على اكتشاف أي ثغرات في نظامها الأمني أو الاكتشاف المبكر لأي خطر يهدد أمن البيانات، وينطبق ذلك على الاستخدامات المشروعة وغير المشروعة على حد سواء. ولذلك تقوم نظم أمن البيانات بالاحتفاظ بسجل لاستخدام البيانات (Log) وبالذات محاولات انتهاك السرية، ومن ثم تخرج هذه النظم التقارير المناسبة مبوبة، إما بالتاريخ أو حسب المستفيد أو مبوبة بالمورد نفسه.

لا تكتفي النظم الأمنية بالتقارير الدورية ولكنها تقوم عند رصد محاولات انتهاك السرية بإخراج رسائل فورية (إلى المستفيد صاحب المورد

أو إلى مسئول أمن النظام أو إلى كليهما معًا)، وفي العـــادة تتضمــن هــذه التقارير بعض المعلومات الإحصائية مثل: تاريخ الواقعة والوقت الذي تمــت فيه وعدد المحاولات التي قام بها المستفيد لارتكاب هذا الانتهاك. ويمكن عن طريق تحليل تلك المعلومات الإحصائية الاستفادة من نتائج هذا التحليل فـــي إحكام السيطرة على أمن الحاسب.

٥-٢- التقارير التي تنتجها نظم الأمن

١) قائمة بالوقائع التي تم تسجيلها في شكل تسهل قراءته وفهمه.

٢) تحديد المحاولات غير المشروعة لاستخدام مــوارد النظــام بحيــث توضح المستفيد الذي قام بهذه المحاولات وعــدد هــذه المحــاولات وتفاصيلها.

٣) قائمة برسائل التحذير إذا كان معمولاً بنظام " فترة الســماح " التـــي تُمنح للمستفيد بشكل مؤقت.

٤) قائمة بالنشاط الذي تم على كل مورد مصنفة حسب مالك المورد.

٥) قائمة بالموارد العامة ومالكيها.

٦) وصف نشاط كل مستفيد وكل مجموعة من المستفيدين.

٧) ملخص لاستخدام النظام وموارده.

٥-٣- التقارير التي تنتجها النظم الرقابية

بالإضافة إلى التقارير التي تخرجها نظم أمن البيانات هناك تقارير أخرى تخرجها النظم الرقابية (Monitoring Systems) التي تراقب المستوى الأمني للنظام. وهذه التقارير الهدف منها تحديد مستوى الأمن في النظام ومنها:

١) تقرير برامج النظام:

ويعطي هذا التقرير قائمة بكل برامج النظام المهمة التي يحتاج المستفيد إلى صلاحيات خاصة لتشغيلها.

٢) تقرير المستفيدين:

ويعطي قائمة بأسماء جميع المستفيدين في المؤسسة وصلاحياتهم، وقائمة بمجموعات المستفيدين والصلاحيات الممنوحة لكل مجموعة من المستفيدين المنتمين إليها، كما يعطي إحصائية بأعداد المستفيدين مصنفة حسب درجة صلاحياتهم.

٣) تقرير الملفات:

ويعطي هذا التقرير قائمة بالملفات المهمة في النظام وبعض البيانات عنها (أسماؤها وأماكن وجودها على الأقراص ودرجة الصلاحية المطلوبة لاستخدام هذه الملفات).

٤) تقرير الإجراءات:

ويعطي هذا التقرير قائمة بالإجراءات المهمة في النظام والتي تقرر المؤسسة ضرورة حمايتها، كما يظهر التقرير المستفيدين المسموح لهم باستخدام هذه الإجراءات.

٥) تقرير تصنيف الموارد العامة:

ويصنف هذا التقرير الموارد العامة ويعطي قائمة بهذه الموارد المصنفة ومستوى الصلاحية العام اللازم لاستخدام كل صنف (Class) من هذه الموارد.

٦) تقرير مراقبة المستفيد:

يعطي هذا التقرير قائمة بنشاط بعض المستفيدين الذين يتطلب الأمر مراقبة نشاطهم.

٧) تقرير مراقبة المورد:

يعطي هذا التقرير قائمة بالنشاط الذي تم على مورد معين لمتابعة واقعة معينة.

٦- بعض نظم أمن البيانات المتوفرة بالأسواق

٦-١- نظم أمن الحاسبات المركزية

بالنسبة لعالم الحاسبات المركزية الكبيرة، لا يوجد الكثير من نظم الأمن في الأسواق وربما كان السبب هو سيطرة بعض الشركات الكبرى على سوق الحاسبات المركزية، وتتميز هذه السوق بضخامة الإنتاج حيث يجب أن تكون نظم الأمن شاملة ومتناغمة مع نظام التشغيل الرئيسي ومع العديد من نظم التشغيل المساعدة، ولذلك تحجم شركات نظم أمن المعلومات الصغيرة عن الدخول إلى هذه السوق وتنفرد بها شركات مثل (آي بي إم).

لذلك نجد على رأس نظم أمن الحاسبات المركزية الشهيرة نظامان:

١) نظام "راكف" (Resource Access Control Facility) (RACF):

ويُستخدم هذا النظام لمراقبة وتنظيم استخدام كافة الموارد في بيئة تشغيل "آي بي إم" ونظم التشغيل الرئيسية فيها مثل (MVS) و (VM) ونظم التشغيل المساعدة مثل نظام الاتصال المباشر (CICS) وغيره وكذلك البرمجيات ونظم إدارة قواعد البيانات المختلفة في هذه البيئة مثل (DB2).

٢) نظام (Access Control Facility II) (ACF2):

ويقوم هذا النظام بنفس أنشطة نظام "راكف" إلا أنه يتفوق عليه في بعض أنواع التقارير المنتجة منه، وكذلك في قدرته على التعامل مع أنظمة ليست من إنتاج شركة "آي. بي. إم".

كما توجد بعض الأنظمة الأخرى الأقل انتشاراً ، بسبب أنها تتعامل مع عدد محدود من نظم التشغيل المساعدة أو نظم قواعد البيانات، مثل نظام (Top Secret) الذي يُستخدم بكفاءة مع بعض نظم قواعد البيانات الشهيرة. ونرى كثيرًا من الشركات المنتجة لنظم قواعد البيانات تفضل إنتاج نظمها الأمنية الخاصة حتى لا يؤثر النظام الأمني (وهو لا بد سيفعل) على الأداء، ومن بين هذه الشركات شركة (أوراكل Oracle).

بسبب محدودية وخصوصية نظم أمن الحاسبات المركزية سنتوسع في الحديث عن نظم أمن البيانات الخاصة بالحاسبات الشخصية.

٦-٢ نظم أمن الحاسبات الشخصية

نعرض فيما يلي بعض نظم أمن البيانات المتاحة في الأسواق والخاصة بالحاسبات الشخصية:

توجد عدة برمجيات في الأسواق تعتبر امتداداً لنظام التشغيل (DOS) ومعظم هذه البرمجيات يدعم تعدد المستفيدين (١٠-٢٠ مستفيدًا) وتتوفر فيها

خصائص تعريف المستفيد والتحقق من شخصيته (عادةً من خلال كلمة مرور)، ويصدر بعض هذه البرمجيات تقارير عن انتهاكات السرية ومحاولات الدخول غير المصرح بها. ومعظم هذه البرمجيات يقوم بتشفير البيانات على أقراص التخزين باستخدام مفاتيح تشفير غير معلومة إلا للبرنامج نفسه فقط. ولتحقيق ذلك يتم استخدام مفتاح تشفير مختلف لكل مستفيد، وعندما يقوم المستفيد بتعريف نفسه يتم تحديد المفتاح المناسب آليًا وبأسلوب مستتر عن المستفيد، وبذلك فإن أي محاولة للاطلاع على البيانات بالالتفاف حول هذا النظام لن تؤدي إلا إلى الحصول على بيانات مشفرة لا معنى لها. ولحماية بيانات المستفيد في حالة ضياع أو نسيان كلمة المرور تعطي معظم هذه النظم لمسئول أمن النظام الحق في تعديل كلمة المرور (وليس معرفتها)، ومن ثم يسمح للمستفيد بإدخال كلمة جديدة.

١) برنامج "بي سي سيف" (PC-safe):

برنامج "بي سي سيف" (PC-safe) والذي أنتجته شركة "إنيجما لوجيك" (Enigma Logic) يستخدم كلمة مرور تستخدم لمرة واحدة فقط لتنظيم استخدام الحاسب فيقدم بذلك أسلوبًا للتحكم في استخدام البيانات يطلق عليه **(التحكم المحمول Portable control)** إذ يمكن نقل البيانات من نظام تشغيل إلى آخر في نفس الصورة المشفرة، ويمكن استخدام البيانات حيث يوجد "**توكن**" كلمة المرور التي تستخدم لمرة واحدة، ولا يشترط أن يكون ذلك من خلال نظام التشغيل الذي تم من خلاله تشفير البيانات بل من خلال أي نظام تشغيل آخر. وهذا البرنامج يتطلب عتادًا خاصًا (H/W) يتيح استخدام كلمة المرور التي تستعمل لمرة واحدة وهذا العتاد محمول هو الآخر.

يسمح برنامج (بي سي سيف) بتشفير البيانات بواسطة المستخدم والاحتفاظ بها في الصورة المشفرة ولا يمنع ذلك من استخدامها من قِبل

مستخدمين آخرين، بافتراض أنهم مصرح لهم بذلك، فعند طلبها من قبل المستخدم الجديد يتم فك تشفير أجزاء البيانات التي يحتاج إليها.

يقاوم هذا البرنامج محاولات اكتشاف كلمة المرور عن طريق التجربة والخطأ لأنه يتوقع كلمة مرور مختلفة في كل مرة، وبذلك فإذا تمكن أحد المستخدمين من اكتشاف كلمة المرور الخاصة بمستخدم آخر فإنها لن تنفعه إذا أراد الدخول بها بعد خروج المستخدم الحقيقي لأن النظام في هذه الحالة سيتوقع كلمة مرور جديدة.

٢) برنامج "إيزاك ٢٢٠٠" (ISAC2200):

يعتبر برنامج "إيزاك ٢٢٠٠" (ISAC2200) من شركة "أيزوليشن سستمز" (Isolation Systems) الكندية امتداداً لنظام التشغيل (DOS) ، وهو يفرض استخدام المواصفات القياسية لوزارة الدفاع الأمريكية فيحتفظ بسجل لكل ملف، أما بالنسبة للبرامج فيقوم البرنامج بتصنيف المستخدمين الذين يحق لهم استخدام كل برنامج ويمنح حق الاستخدام فقط للمستخدمين الذين تنطبق عليهم شروط الصلاحية المحددة بهذا السجل. وهذا البرنامج يعمل مع كل من نظام (DOS) ونظام (UNIX).

٣) برنامج "ديسك ووتشر" (Disk Watcher):

البرنامج "ديسك ووتشر" هو واحد من مجموعة من المنتجات التي صممت لحماية البيانات ولضمان ألا يتم محوها عن طريق خطأ غير مقصود من جانب المستخدم، فيقوم هذا البرنامج على سبيل المثال باستبدال الأمر (FORMAT) وهو أحد أوامر (DOS) ويضع مكانه أمرًا آخر يتطلب تأكيدًا من المستخدم عند استخدامه. وهذا البرنامج يحتاج بصفة عامة إلى تأكيد عند أي محاولة من جانب أي برنامج للكتابة فوق أي بيانات موجودة من قبل. وهو بذلك يقاوم أي فيروس يحاول تعديل البيانات أو محوها أو

إتلافها، ومعنى ذلك أن هذا البرنامج يعمل بعد أن يبدأ الفيروس عمله لمنعه من تحقيق أغراضه، ولكن ذلك لم يمنع مطوري الفيروسات من تصميمها بحيث تستطيع التعرف على وجود برنامج "ديسك ووتشر" وتخطيه.

٤) برنامج "ميل سيف" (Mailsafe) :

يقوم برنامج "ميل سيف" من شركة (RSA Data Security) بتشفير الملفات من أجل تأمين الاتصالات وحالات التشارك في البيانات. وبرغم أن هذا البرنامج واسع الانتشار حاليًا في كثير من الاستخدامات، فإنه أكثر نفعًا وجاذبية في حالات البريد الإلكتروني فهو يتيح ما نطلق عليه (أغلفة رقمية Digital Envelopes) و (توقيعات رقمية Digital Signatures). أما الأغلفة الرقمية فهي تخفي المعلومات عن الجميع ماعدا الجهة المقصود وصول الرسالة إليها، بينما التوقيعات الرقمية فهي تنسب الرسالة إلى مرسلها الحقيقي وتمنع أي تغييرات غير مرخص بها على الرسالة ، وهاتان النقطتان تحاكيان تمامًا ما نقوم به في تأمين الرسائل اليدوية.

٥) برنامج "سيرتوس" (Certus):

يعتبر نظام "سيرتوس" الامتداد الأمني لنظام التشغيل (DOS) ، ولكن الهدف منه ليس تنظيم استخدام البيانات ولكن منع النظام من تنفيذ برامج دخيلة أو غير مرخص بها، فيمكن بذلك استخدامه للحماية من البرمجيات المدسوسة والتي قد تحتوي على فيروسات أو أي برنامج دخيل من التي يطلق عليها "حصان طروادة". ويحقق هذا البرنامج ذلك عن طريق فحص اسم أي برنامج تجري محاولة تنفيذه للتأكد من وجوده ضمن قائمة البرامج المجازة والمحفوظة لديه مسبقًا. ولضمان سلامة هذا الإجراء فإن البرنامج يذهب إلى أبعد من مجرد التأكد من الاسم فهو يقوم بحساب مجموع اختباري لكل من هذه البرامج مسبقًا، ثم يعيد حساب هذه القيمة للبرنامج موضع

الاختبار قبل السماح له بالتنفيذ للتأكد من حق البرنامج في التنفيذ كأن يتم حساب عدد مرات التشغيل التي يتم تنفيذ هذا البرنامج فيها ومقارنتها بحد أقصى لا يجب أن يتجاوزه عدد مرات التشغيل في اليوم أو في الساعة أو الدقيقة مثلاً.

والبرنامج بذلك لا يمنع فقط تشغيل برامج الفيروسات ولكنه أيضًا يمنع تكرار هذه الفيروسات وتضاعفها وانتشارها، وهذه هي المزية الأساسية لهذا البرنامج إذ إنه يفقد الفيروس أهم أسلحته وهي الانتشار.

٦-٣- نظم الأمن والتشغيل

- **خادم الملفات في الشبكات المحلية**

(LAN Server Access Control):

يتشارك الكثير من مستخدمي نظام التشغيل (DOS) مع المستخدمين الآخرين في البيانات أو في القرص الصلب وذلك من خلال خادم الملفات في الشبكة المحلية. يعني ذلك وجود عدة نسخ من نظام التشغيل (DOS) (نسخة لكل مستخدم بالإضافة إلى نسخة خادم الملفات) وتكون كل نسخة من نظام (DOS) معزولة عن النسخ الأخرى لوجودها في جهاز مستقل وبذلك يتحقق مبدأ العزل، ويقوم خادم الملفات بتحقيق التوازن في التشارك في الاستخدام بين الحاسبات الشخصية المشتركة في الشبكة وذلك بأن يتدخل النظام عند اكتشافه وجود (Loop) تسبب فيها أحد الأجهزة مما يجعل هذا الجهاز يستحوذ على أحد الموارد فيقوم النظام بإخراج هذا الجهاز من الخدمة مؤقتًا، وكذلك باستخدام أسلوب "توكن" (Token) في الشبكات المحلية الحلقية من نوع (Token Ring) بحيث تتم الاستجابة للوحدات المشتركة في الشبكة في حالة احتياجها للخدمة ، وذلك بالمرور عليها بصفة دورية. وهذا في حد ذاته يعتبر نظامًا آمنًا متعدد المستفيدين برغم أن كلاً من المستفيدين يستخدم نظام

تشغيل فردي غير آمن في حد ذاته. ومن أجل تحقيق ذلك يجب أن تتولى برمجيات خادم الملفات مسئولية الأمن التي ذكرناها من قبل، وتقوم معظم البرمجيات التي تشغل خادم الملفات بذلك فتحمي نفسها من تدخل المستفيدين.

وعن طريق استخدام أكثر من معالج (Multiple processors) يمكن تحقيق مبدأ عزل العمليات (Processes) فيحدث الاتصال بين المعالجات عند تنفيذ العمليات فقط. ولا يهم أن يستخدم خادم الملفات نظام تشغيل غير آمن في حد ذاته مادام مستخدمو خادم الملفات أنفسهم لا يستخدمون إلا تطبيقات خادم الملفات فقط وليست لديهم القدرة على رؤية أو تعديل نسخة (DOS) الموجودة على خادم الملفات مثلما هو الحال في الشبكات التي تتضمن حاسبات شخصية بدون وحدات إدارة أقراص والتي تكون عند تشغيلها تحت إدارة نظام تشغيل الشبكة فقط، فيتم عرض قائمة تطبيقات (Menu) على المستفيد بمجرد تشغيله للجهاز ليختار منها التطبيق المطلوب، وفي هذه الحالة يكون المستفيد مقطوع الصلة بنظام التشغيل (DOS) الموجود على خادم الملفات.

وكما هو الحال مع نظم تشغيل الحاسبات الكبيرة فإنه من الضروري تقييد حق التعديل على نسخ نظام التشغيل التي تقع في الذاكرة الثانوية (على الأقراص). ولأن نظام التشغيل الخاص بخادم الملفات يتم تخزينه في فهرس خاص شأنه شأن باقي الحاسبات المتصلة به ، فإن المستفيدين يمكنهم التعديل عليه ولكن في حدود بحيث لا يمكنهم إجراء تعديلات جوهرية قد تؤثر على كفاءة وظائف نظام التشغيل.

٦-٤- برامج تحقق ضوابط استخدام الحاسبات الشخصية

هناك برامج كثيرة في الأسواق تحقق ضوابط الاستخدام في الحاسبات الشخصية ومعظمها يستطيع منع المستخدم العادي (عامل النظافة في

المؤسسة مثلاً) من استخدام الحاسب الشخصي الموجود في المكتب، ولكن المستخدم الأكثر دراية لن توقفه هذه النظم البسيطة فهو قد يستخدم أدوات مثل برنامج "نورتون" مثلاً للالتفاف حول نظام الحماية المستخدم. وربما كان المقتحم على مستوى أعلى فقد يكون منظمة دولية أو محترفًا متخصصًا في اختراق الحاسبات يعرف جيدًا ما الذي يبحث عنه وكيف يتعامل معه، وللأسف لا توجد حتى الآن الوسيلة المثلى لحماية الحاسب الشخصي من مثل هذا الخطر. ولكن من أجل تقليل فرص نجاح مثل هذا الاختراق يجب تصميم برنامج الأمن جيدًا فيجب مثلاً أن يستخدم نظام تشفير قويًا مع حسن اختيار مفتاح التشفير، وهذه النظم يجب ألا تعتمد على رقم المستفيد وكلمة المرور فقط، ولكنها يجب أن تستخدم كذلك التقنيات الحديثة مثل: تقنيات (البيولوجيا الإحصائية Biometric techniques) و(البطاقات الذكية Smart cards).

وتعتبر أضعف النقاط في عملية ضبط استخدام الحاسبات الشخصية هي في الحقيقة المستفيد نفسه وليست البرمجيات التي تعمل على ضبط الاستخدام، فهذا المستفيد هو الذي قد يكتب كلمة المرور ثم يتركها في مكان ظاهر، وهو الذي قد ينسى بطاقته الذكية على المكتب، وهو الذي قد يترك حاسبه الشخصي مفتوحًا، ولذلك يعتبر تعليم وتدريب المستفيد من أهم قواعد تأمين الحاسبات.

وبصفة عامة فإن الحاسبات التي تعتمد على استخدام العتاد (H/W) في الأمن تكون أكثر أمنًا من التي تعتمد على استخدام البرمجيات، ولكنها أغلى ثمنًا وأصعب في التركيب.

٧- المفاضلة بين نظم أمن البيانات

عند اختيار نظام أمني للحاسب الشخصي (سواء كان برنامجًا أو عتادًا) يجب مراعاة النقاط التالية وهي التي تشكل أساس المفاضلة بين هذه النظم:

١) يجب على النظام أن يمنع تشغيل الحاسب من القرص المرن حتى لا يمكن تجنب نظام الأمن.

٢) يجب تمييز جميع المستفيدين عن طريق رقم المستفيد وكلمة المرور معًا، ولا يجب عرض كلمة المرور على الشاشة عند إدخالها، ويجب أن يفرض النظام حدًا أدنى لعدد حروف كلمة المرور (٦ أو ٨ حروف مثلاً).

٣) يجب أن يكون لكلمات المرور تاريخ انقضاء بحيث يضطر المستفيد إلى تغييرها من آن لآخر وألا يسمح النظام بإعادة استخدام كلمة المرور مرة أخرى أو استخدام الكلمة التي سبقتها.

٤) يجب أن يتم فصل الساعة التي تعطي الوقت والتاريخ عن ساعة نظام التشغيل (DOS) وإلا أصبحت النظم التي تسمح بالاستخدام خلال أوقات معينة غير ذات فائدة إذ إن أي شخص يستطيع تعديل الوقت والتاريخ في نظام (DOS) وهذا الأسلوب يحتاج إلى وجود عتاد معين.

٥) يجب أن تخصص للمستفيد أوقات معينة في اليوم وأيام معينة في الأسبوع يسمح له فيها بالاستخدام، حيث يمنع ذلك الزائر الليلي الذي يعرف كلمة المرور من الوصول إلى البيانات.

٦) يجب أن تحدد بدقة لكل مستفيد مجموعة الصلاحيات الممنوحة له مثل أيُّ الفهارس يُسمح له بالدخول إليها وأيُّ البرامج يُسمح له بتشغيلها، وهكذا، كما يجب أن يقوم النظام الأمني بمراقبة ذلك.

٧) إذا كانت الحاسبات الشخصية تستخدم لنقل الملفات من وإلى الحاسب الكبير فيجب أن تحدد بدقة صلاحيات استخدام الملفات.

٨) يجب الاحتفاظ بسجل يبين مَن من المستخدمين قد دخل إلى النظام؟ ومتى كان ذلك؟ ويجب أن يكون هذا السجل مشفرًا ولا يمكن محوه أو تعديله.

٩) يجب أن يكون في مقدور المستخدم أن يترك حاسبه الشخصي مغلقًا بحيث لا يمكن أن يفتح إلا بواسطة كلمة مرور صحيحة، كما يجب أن يتم إظلام الشاشة عند إغلاق الحاسب، فلا تبقى المعلومات السابق عرضها على الشاشة معروضة بل يتم محوها مما يمكن المستفيد من أن يذهب للغداء مثلاً دون خوف من أن يعبث أحد بالحاسب الشخصي الخاص به.

١٠) يجب أن يكون في مقدور المستخدم أن يجعل الشاشة تظلم بمجرد النقر على مفتاح واحد، وبذلك يمنع أي مشاهد من رؤية البيانات السرية المعروضة على الشاشة.

١١) يجب أن يحتوي النظام على وظيفة إغلاق الحاسب آليًا إذا لم يتم استخدام لوحة المفاتيح لفترة زمنية معينة، وفي هذه الحالة فحتى لو ترك الحاسب مفتوحًا فإنه سيقوم بإغلاق نفسه آليًا.

١٢) ضرورة وجود مجموعة من البرامج الصغيرة التي تساعد مسئول أمن المعلومات كأن تسهل إنشاء أرقام مستخدمين جدد أو تساعد على تعديل الصلاحيات وغير ذلك، وبحيث تساعد المستخدم على تغيير كلمة المرور الخاصة به بحيث لا يتمكن مسئول النظام من الاطلاع على كلمات المرور الخاصة بالمستفيدين، وإنما يكون إدخالها وتعديلها من مسئولية المستخدم وحده.

١٣) يجب توفير وظيفة التشفير الآلي للملفات الحساسة، ويجب أن يكون ذلك باستخدام خوارزميات تشفير معترف بها مثل خوارزمية (DES)،

أو خوارزميات أكثر سرعة إذا لزم الأمر ولكن بعد تدقيقها بواسطة مؤسسة أمينة محايدة.

١٤) من الضروري ألا يتعارض النظام الأمني سواء مع نظام التشغيل أو مع العتاد وهذه النقطة تكتسب أهمية خاصة لأن النظم الأمنية عادة ما تتغلغل في نظام التشغيل مما قد ينجم عنه مشاكل عند الاستخدام.

١٥) يجب أن يتم تحديد العبء الناشئ عن النظام الأمني (Overhead) والذي يتناسب تقريبًا مع عدد المستخدمين الذين يستخدمون نفس الجهاز، فإذا زاد هذا العبء عن الحد المقبول يجب أن يؤخذ في الاعتبار البديل الآخر وهو استخدام شبكة محلية تحتوي على عدة حاسبات شخصية (محطات عمل) بحيث لا تحتوي محطات العمل هذه على وحدات لإدارة الأقراص.

٨- أسلوب النسخ الاحتياطي ومعدلاته

٨-١- النسخ الاحتياطي

يعتبر النسخ الاحتياطي (Back-up) أحد الأركان الأساسية لأمن البيانات والمقصود به أخذ نسخة من البيانات وتخزينها في مكان آمن، وعند الحاجة يتم استرجاع هذه البيانات (Restore) بمعنى استعادة محتويات النسخة الاحتياطية لتكون هي النسخة العاملة حتى يمكن إعادة تشغيل النظام من النقطة التي تم أخذ النسخة الاحتياطية عندها. ويعتبر النسخ الاحتياطي إجراءً احتياطيًا ليس إلا، فلو كان نظام تأمين الحاسب كفؤًا بنسبة ١٠٠% لما كان هناك داعٍ له، ولكن المؤكد أنه بسبب ضعف إجراءات التأمين أو بسبب أخطاء البشر الذين لا يلتزمون بها تأتي لحظة ما يحدث فيها تلف للبيانات أو

الملفات وتظهر الحاجة إلى النسخ الاحتياطية فنسترجعها ونبدأ عملية إعادة تنفيذ التعديلات التي تمت على البيانات منذ اللحظة التي سبق أن أخذت فيها النسخة الاحتياطية.

٨-٢- معدلات إنتاج النسخ الاحتياطية

١) يجب أن يكون النسخ الاحتياطي جزءاً من الروتين اليومي لمركز الحاسب فيتم تنفيذه في أوقات محددة ولا يترك تنفيذه لرغبة المشغلين أو لتقديرهم، ولذلك لابد أن يكون "**دوريًا**" وفي يوم معلوم من الأسبوع أو في ساعة محددة من اليوم، لأنه عند حدوث الخطأ يلزم معرفة إلى أي مدى يجب الرجوع إلى الوراء لاستعادة البيانات.

٢) يمكن أن تأخذ النسخ الاحتياطية عدة أشكال طبقًا لاحتياجات المؤسسة، إذ إن الهدف هو أنه في حالة حدوث الخطأ يجب إعادة الملفات إلى ما كانت عليه تمامًا وقت حدوث الخطأ، على ألا تزداد عمليات النسخ الاحتياطي بشكل يؤثر على إنتاجية النظام.

٣) النسخ الاحتياطي يمكن أن يكون إما على مستوى الملف أو على مستوى القرص الممغنط بالكامل، أي إنه إما أن يكون على أساس منطقي (Logical) أو على أساس مادي (Physical)، فنسخ قرص بالكامل قد يكون أكثر سرعة ولكن ذلك يتطلب معرفة البيانات الموجودة على كل قرص للتأكد من وجود جميع الملفات المطلوب نسخها على القرص. وبالإضافة إلى نسخ الأقراص ربما كان من الضروري الحصول على نسخ احتياطية لملفات معينة على فترات أكثر تقاربًا، كالملفات النشطة

جدًا أو الملفات الحساسة. فبالنسبة للملفات النشطة يجب أن يتم في خلال الفترة بين النسخ الاحتياطية المتتالية، إعداد نسخ أخرى تتضمن التغييرات التي قد تطرأ على الملف في الفترة بين عمليتي النسخ الاحتياطي (Incremental backups)، وعند استعادة الملف يتم أولاً استعادة النسخة الاحتياطية الأخيرة ثم استعادة التغييرات.

٤) يعتمد معدل إنتاج النسخ الاحتياطية على النظام المطلوب حمايته، فيتم عادة أخذ النسخة الاحتياطية إما قبل، أو ربما بعد إجراء دفعة التعديلات (Batch updates). أما في حالة النظم التي يتم تعديلها بشكل مباشر (Online) فيتم أخذ النسخ الاحتياطية على فترات محددة سلفًا بحيث تكون المعاملات التي تتم بعد أخذ النسخة الاحتياطية قليلة بما يسمح بإعادة تنفيذها، فالنظم التي يزداد فيها معدل المعاملات أو تلك التي يلزم أن تكون معلوماتها حديثة باستمرار فإنها تحتاج إلى معدلات متقاربة للنسخ الاحتياطي.

٥) عادة ما تؤخذ النسخ الاحتياطية على فترات ثابتة، ولكن هناك ما يعرف بالنسخ الاحتياطي المستمر (Continuous Back-up) وهو يتم باستخدام أقراص "متماثلة" (Mirror disk) أو (Shadow disk) تكون نسخة مطابقة من القرص الأصلي، وكلما تم تعديل على القرص الأصلي يتم إجراء نفس التعديل على القرص المماثل.

٦) ويلاحظ أنه إذا كان كلا القرصين موجودان في نفس غرفة التشغيل فإن هذا الأسلوب لا يكون مفيدًا إلا في حالة تعطل أحد الأقراص فيمكن أن يحل الآخر محله، أما إذا كانت المشكلة أعم وتشمل غرفة الحاسب كلها

فإن هذا الإجراء لن يفيد. ولذلك تعمد بعض المؤسسات إلى وضع القرص المماثل في مكان بعيد، وقد يكون كذلك متصلاً بالحاسب البديل.

٧) هناك بعض حالات خاصة من النسخ الاحتياطي منها حالة الملف شبه الثابت الذي لا يتم تعديله إلا على فترات متباعدة، ففي هذه الحالة لا معنى لأخذ النسخة الاحتياطية بصورة متكررة حيث لا يتم أي تعديل على الملف، ولذلك يتم تحديد دورية النسخ الاحتياطي بشكل متغير، ففي الفترات الميتة تؤخذ كل شهرين مثلاً وفي الفترات النشطة تؤخذ على فترات أقصر.

٨) هناك أيضًا حالة الملف التاريخي (Archive File) وهو لا يعتبر في الحقيقة نسخة احتياطية إذ ليس الهدف منه أن تحل هذه النسخة محل نسخة تالفة وإنما الهدف منه الاحتفاظ بالنسخة كمرجع ولذلك فهي تؤخذ في نهاية كل عام مثلاً لأغراض التحليل أو للرجوع إليها للمراجعة والتدقيق أو الإحصاء.

٨-٣- وسائط النسخ الاحتياطية

١) يتم في العادة الاحتفاظ بالمستندات الورقية المستخدمة خلال الفترات الواقعة بين عمليات النسخ الاحتياطي في خزائن مقاومة للحريق حتى يمكن استخدامها لإعادة إدخال المعاملات بعد استرجاع البيانات من نسخة احتياطية سابقة والعودة إلى وضع ما قبل هذه المستندات الورقية.

٢) يكثر استخدام الشريط الممغنط (وبخاصة الكارتردج) كوسط يمكن أخذ النسخ الاحتياطية عليه لصغر حجمه وسهولة التعامل معه وتخزينه ونقله، ولكن الأشرطة تكون عرضة للتلف بمرور الزمن ولذلك يجب إعادة كتابة البيانات الموجودة على الأشرطة كل عام.

٣) يمكن استخدام الأقراص الممغنطة لحفظ النسخ الاحتياطية، ولكي يصبح استخدامها ذا فائدة ملموسة يجب أن تُحفظ هذه الأقراص في مكان بعيد بما لا يقل عن كيلومترين من مكان القرص الأصلي.

٤) وبالنسبة للحاسبات الشخصية فإنها تستخدم الأقراص المرنة كوسط لتخزين النسخ الاحتياطية، ولكنها بطيئة للغاية خاصة في حالة الأحجام الكبيرة من البيانات، كما أنه لا يمكن الاطمئنان إليها بعد مرور فترة طويلة من الزمن، ولذلك يجب إعادة تسجيل البيانات عليها كل ستة أشهر. وكثيرًا ما تستخدم الأشرطة الممغنطة للتخزين في الحاسبات الشخصية.

٥) تعتبر الأقراص الضوئية (CD-ROM's) أحد الوسائط المنقولة المناسبة للنسخ الاحتياطي، ولما كانت بعض أنواعهاغير قابلة لإعادة الكتابة عليها فهي لذلك تعتبر أكثر أمانًا، بالإضافة إلى كونها أرخص نسبيًا وتعيش مدة أطول.

٦) كقاعدة عامة فإن جميع البيانات المخزنة احتياطيًا (باستثناء الأقراص الضوئية) لابد من إعادة كتابتها على فترات لا تزيد عن العام.

٨-٤- التأكد من سلامة النسخ

١) من المهم جدًا التأكد من أن هذه النسخ الاحتياطية التي تستمر المؤسسة في إعدادها وترتيبها وتخزينها هي نسخ سليمة وصالحة للعمل، ولذلك لابد من إضافة إجراءات تدقيق في برنامج النسخ الاحتياطي مثل: حساب عدد السجلات ومقارنته بالنسخة الحالية للتأكد من سلامة هذه النسخة.

٢) قد يكون من الضروري تعدد النسخ الاحتياطية للقرص الواحد أو الملف الواحد، إذ ربما لا تتم عملية النسخ الاحتياطي على الوجه المرضي، وقد تفسد النسخة ويفسد الأصل كذلك، ولذلك فوجود نسخة ثالثة أمر مفيد في مثل هذه الأحوال. وعادة يُستخدم ما يسمى دورة النسخ حيث يتم الاحتفاظ بعدة نسخ زمنية ــ خمس نسخ مثلاً ــ وعند أخذ النسخة الاحتياطية الجديدة يتم أخذها على النسخة الأقدم بحيث يكون لدينا باستمرار خمس نسخ من البيانات يفصل بينها يوم أو أسبوع أو شهر، ويتوقف هذا الفاصل على معدل وكثافة تعديل البيانات المنسوخة.

٣) لا يجب التوقف عند نسخ البيانات فقط ولكن من المهم كذلك نسخ البرامج التي تتعامل مع البيانات فبدونها لا تكون للبيانات قيمة، ويتم نسخ البرامج إما على فترات ثابتة أو كلما حدث تغيير ملموس فيها، كأن يتم تطوير نسخة جديدة من التطبيق. في هذه الحالة يتم إعداد نسخة احتياطية من (مكتبة البرامج الإنتاجية Production library). وحتى بالنسبة (لمكتبة البرامج التجريبية Test library) فإنها أيضًا

يجب نسخها دوريًا، إذ ربما يمسح المبرمج بالخطأ أحـــد برامجـــه أو يجري عليه تعديلات قد تتلفه، وفي هذه الحالة قد يكون من المطلـــوب إعادة البرنامج إلى الصورة التي كان عليها قبل يوم أو يومين أو ربما أسبوع. وبالنسبة لنظم التشغيل فعند تركيب نظام تشغيل جديد ـــ مثـــلاً ـــ فمن الضروري الاحتفاظ بنسخة من النظام السابق.

٩- استعادة البيانات المفقودة

٩-١ إجراءات الاستعادة

١) يجب لضمان نجاح استرجاع البيانات المفقودة أن يتم تخزين النســـخ الاحتياطية في مكان آمن، ويتـــم اســـترجاع البيانـــات المخزنـــة (أو البرامج) عند الحاجة بواسطة برامج مساعدة جاهزة (Utilities) .

٢) يجب توعية المشغلين بالإجراءات الواجب اتباعـــها لتنفيـــذ عمليـــات الاسترجاع بالشكل الصحيح، فهذه العمليات لا تتم بصفة دورية مثـــل النسخ الاحتياطي، وإنما تتم عندما تكون هناك حاجة إليـــها، وتظـــهر الحاجة إليها في حالات الكوارث أو على الأقل لمعالجـــة الأخطـــاء. ويجب أن تتضمن التعليمات الثابتة في غرفة التشغيل الإجراءات التـــي يتعين على المشغلين اتباعها لاسترجاع الملفات التالفة.

٩-٢ التأكد من سلامة الاستعادة

١) يجب إجراء اختبارات من وقت إلى آخر بهدف التأكد من أن البيانات والبرامج التي تم نسخها احتياطيًا يمكن استرجاعها بنجاح ، ويمكن من خلال هذه الاختبارات استرجاع (Restore) البيانات ثم عد السجلات التي تمت استعادتها وحساب مجموع بعض الحقول واختيار بعض السجلات عشوائيًا لمطابقتها مع السجلات الأصلية.

٢) ومن المهم أن نلاحظ أن عملية الاسترجاع لا يجب أن تتم بحيث تحل محل البيانات الأصلية وذلك تحسبًا لفشل عملية الاسترجاع، فلو أنها فشلت فسوف يتم محو البيانات الأصلية مع عدم استرجاع النسخة الاحتياطية مما يؤدي إلى ضياع البيانات بالكامل.

١٠- مستويات الأمن في مراكز الحاسب

حددت وزارة الدفاع الأمريكية مواصفات قياسية للأمن بالنسبة لنظم الحاسب الخاصة بالدوائر الحكومية في الولايات المتحدة بصفة عامة. وتقوم الوزارة بتقويم أي نظام من ناحية الأمن ثم يُصنف وفقًا لدرجة أخذه بأسباب الأمن ومدى اتباعه للمعايير الأمنية وكفاءته في حماية موارده.

ووفقًا لهذه المواصفات فهناك مستويات عدة للأمن بعضها من الفئة "أ" وبعضها من الفئة "ب" وبعضها من الفئة "ج" وفقًا للكتاب البرتقالي الذي أصدرته وزارة الدفاع الأمريكية في عام ١٩٨٥م ثم حدثته بعد ذلك في أعوام ١٩٨٨م و ١٩٩١م وسنختار منها مستويين متميزين:

١٠-١- مستوى الأمن ج٢ (C2 security level)

وينطبق هذا المستوى على نظام الحاسب الذي يفرض ضوابط لاستخدام البيانات تميز بين المستفيدين بحيث يكون لكل مستفيد رقمه الخاص وتتم متابعة وتنظيم استخدام كل مستفيد لموارد الحاسب وذلك من خلال استخدام عدة إجراءات مثل إجراءات الدخول إلى النظام (Logon Procedures) ومراقبة أي أحداث تمس أمن الحاسب، وكذلك من خلال أسلوب عزل الموارد (Resource Isolation) الذي يضمن إحكام السيطرة على استخدام هذه الموارد.

١٠-٢- مستوى الأمن ب١ (B1 security level)

في هذا المستوى (وهو الأعلى) تأخذ وزارة الدفاع الأمريكية في الاعتبار نقطتين رئيسيتين هما: السياسة الأمنية، وتحديد المسئولية.

١) **السياسة الأمنية:**

عرفتها الوزارة باعتبارها مجموعة القواعد أو الممارسات التي تنظم الكيفية التي تتعامل بها المؤسسة مع بياناتها الحساسة.

٢) **تحديد المسئولية:**

ويتطلب ذلك تحديد الصلة بين كل إجراء والمستفيد المسئول عن تنفيذ هذا الإجراء.

فالسياسة الأمنية التي يتم تطبيقها في بيئة مستوى الأمن (ب١) تحتاج في المقام الأول إلى نظام دقيق لضبط استخدام الموارد بحيث أنه لا يقوم فقط بمنع الأفراد من استخدام المعلومات التي تحتاج إلى درجة صلاحية أعلى من صلاحياتهم، ولكنه أيضًا يمنع هؤلاء الأفراد من الالتفاف حول النظام بإلغاء الحظر المفروض على هذه المعلومات. فالنظام يجب أن يكون قادرا على

حماية الموارد ذات المستويات المختلفة من الحساسية، وأن يكون قادراً على تتبع أي استخدام غير مشروع للبيانات للوصول إلى المسئول عن ذلك.

إن نظم الحاسب الموثوق بها هي التي تستخدم كلاً من العتاد (Hardware) والبرمجيات (Software) للتأكد من تحقق هذه الشروط.

الفصل الحادي عشر

أمن التطبيقات

موضوعات الفصل:

(١) بيئة العمل.

(٢) المشاكل الأمنية في بيئة العميل / الخادم.

(٣) تأمين التطبيقات.

(٤) استخدام التطبيقات بواسطة الأجهزة المحمولة.



نتناول في هذا الفصل موضوع "أمن التطبيقات"، وهو من أهم الموضوعات في أمن المعلومات المحفوظة على الحاسب، ثم نتلوه بفصل عن أمن قواعد البيانات، والموضوعان متلازمان ويهمان كل مبرمج للحاسب الآلي. نبدأ الفصل بالحديث عن بيئات العمل المختلفة وأثر اختلاف بيئة العمل على الأمن، ثم نركز على بيئة العميل/الخادم، فنتحدث عن المشكلات الأمنية في هذه البيئة. ننتقل بعد ذلك إلى كيفية تأمين التطبيقات، ونقدم بعض الحلول لبعض مشكلات أمن التطبيقات. ونختتم الفصل بمشكلة مستخدمي التطبيقات الذين يستخدمون الأجهزة المحمولة.

١- بيئة العمل

تتركز معظم مشاكل أمن التطبيقات ــ كقطاع من أمن المعلومات ــ في تنظيم صلاحيات المستفيدين التي يجب التأكد منها قبل السماح لهم باستخدام هذه التطبيقات، والأمر في بيئة الحاسب المركزي يتطلب برامج أمنية مثل: (RACF)، أو (ACF2).

١-١- أثر اختلاف بيئة العمل

عملية المشاركة في الموارد المادية والمنطقية كثيرًا ما تكون مقصورة على البيئات التي تستخدم نظم تشغيل متجانسة مثل: "دوس" و"نوفيل" و"أو إس ٢" و"إن تي" و"أو إس ٤٠٠"، ولكن التشارك بين بيئات عمل تستخدم نظم تشغيل مختلفة ليس من السهل أن يتم بشفافية، ولكنه قد يحتاج إلى تعديلات في البرامج. فمثلاً على عكس الوصول إلى الملفات المشتركة الموجودة على شبكة واحدة تستخدم نظم تشغيل متجانسة، فإن الوصول إلى قاعدة بيانات (دي بي ٢ DB2) في نظام (إم في إس MVS) من بيئة عمل لا تستخدم نظام التشغيل نفسه لا يمكن أن تتم مباشرة من جانب طالب البيانات بنفس السهولة التي يتم بها ذلك من داخل بيئة تشغيل متوافقة. ولكن

الأمر يتطلب معونة نظام التشغيل لإتمام الوصول إلى قاعدة البيانات. ومن المستحيل بالطبع أن يتم إنتاج نظام تشغيل (سوبر) يستطيع التعامل مع "جميع" نظم التشغيل الأخرى وإن كان هذا ممكنا فالتكلفة العالية جدًا تجعله غير ممكن! وليس ببعيد محاولة شركة "صن" إنتاج لغة البرمجة التي تعمل في جميع البيئات، وهي لغة (جافا Java) ولكن المشروع لم يثبت النجاح المنتظر نظرًا لبطء الأداء الناشئ عن الأعباء الكثيرة التي توضع على نظام التشغيل كي يستطيع التعامل مع البيئات المختلفة. ولكن عالم اليوم، خاصة بعد دخول عصر الإنترنت يحتاج بشدة إلى تبادل التعامل بين بيئات العمل المختلفة. وربما كان مفهوم "العميل / الخادم" نفسه نشأ من خلال هذه الحاجة الملحة لوجود جهاز كبير يخدم مجموعة من الأجهزة الأخرى الصغيرة، وفي بيئة "العميل / الخادم" يمكن أن يقوم كل جهاز بدور العميل أو بدور الخادم [Park-1995]. ففي بيئة "العميل / الخادم" لإدارة البيانات مركزيًا يكون هناك خادم واحد يتولى تقديم الخدمة لعملاء كثيرين، بينما في بيئة العميل / الخادم لإدارة البيانات الموزعة يكون كل جهاز خادمًا وعميلاً في الوقت نفسه. ولذلك فكل جهاز عميل يجب أن تكون لديه القدرة على تكوين الطلب وتوجيهه إلى الخادم المناسب بغض النظر عن نوع الخادم أو نظام تشغيله. ويسهل كثيرًا من مهمة العميل أن يكون الخادم قادرا على فهم لغة قياسية مناسبة مثل (لغة الاستفسار البنائية SQL)، وكل خادم من ناحيته يجب أن يكون قادرا على تنفيذ كل مهمة بطريقة تناسب الطلب الموجه إليه.

١-٢- بيئة العميل / الخادم

نظرًا لانتشار بيئة عمل (العميل / الخادم Client / Server) ، ونظرًا لأن تحقيق أمن التطبيقات في هذه البيئة أصعب كثيرًا من بيئة الحاسب المركزي فإننا سنركز على هذه البيئة والحلول التي سنقدمها هنا تصلح لأن يؤخذ بها في بيئة الحاسب المركزي.

يمكن تعريف "الحوسبة" في بيئة "العميل / الخادم" بأنها تتضمن أي جهازي حاسب (أو أكثر) يتم استخدامهما معًا وبشكل متزامن لإنجاز مهمة معينة. ومن أمثلتها استخدام حاسب مركزي يحتوي على قاعدة بيانات ويقوم بتقديم البيانات لمن يريدها، ويحتاج المستفيد لأداء عمله إلى استخدام تطبيقات عديدة، وهذه التطبيقات قد تكون موجودة على حاسب آخر. هذا الحاسب المركزي (خادم قاعدة البيانات) مهمته هي تقديم بيانات دقيقة وحديثة مركزيًا لأي شخص تكون لديه الصلاحية للحصول عليها، أما العميل فمهمته هي معالجة هذه البيانات وفقًا لقواعد محددة من خلال تطبيقات معينة، ثم يتولى عرض المعلومات المطلوبة في الشكل المناسب على شاشة المستخدم.

المشاكل الأمنية في بيئة العميل / الخادم تتضمن بصفة عامة ثلاثة مسائل أساسية هي؛ أولاً: قدرة تطبيقات العميل على أن تحدد احتياج طالب البيانات، وثانيًا: أن تقدم له المعلومات الضرورية فقط دون غيرها، وفي النهاية تأمين البيانات المستقبلة بعد وصولها بالشكل المناسب. هناك اعتبار آخر يختص بالتطبيق الموجود على جهاز العميل وهو قدرة هذا التطبيق على تخزين البيانات المستقبلة من الخادم وتقديم مجموعة مكافئة من المهام للمستفيدين الذين لا يستطيعون الاتصال بجهاز الخادم لوجودهم على الطريق مثلاً أو في الطائرة، فتخزين البيانات على جهاز العميل في حد ذاته لا يشكل مشكلة أمنية كبيرة ولكن سرقة حاسب دفتري (Note Book) من المستفيد (العميل) مع ما يحتويه من معلومات هي المشكلة الحقيقية.

١-٣- مفاهيم لابد منها

هناك خلط بين بيئة (العميل / الخادم Client / Server) وتقنيات أخرى مثل (إدارة البيانات الموزعة Distributed Data Management) و (المعالجة الموزعة Distributive Processing) أو (المعالجة التعاونية Cooperative Processing).

فأما تقنية إدارة البيانات الموزعة (DDM) فهي تتيح الوصـــول إلـــى قاعدة البيانات المطلوبة بغض النظر عن موقعها ودون أن يحتاج المستفيد أن يحدد مكان هذه البيانات وهل هي في جدة أم الرياض أم الدمـــام. والفـــرق الرئيسي هنا بين الوصول للبيانات باستخدام تقنية إدارة البيانـــات الموزعـــة (DDM) أو في بيئة العميل / الخادم (C/S) هو أنه من خلال إدارة البيانـــات الموزعة توجد كينونة منطقية واحدة هي التي تتحكم في جميع العمليات بـدءاً من عملية الوصول للبيانات مروراً بانتقاء هذه البيانات وفي النهاية وصـــولاً إلى معالجة هذه البيانات. فدور الحاسب المضيف لهذه البيانات في هذه الحالة لا يتعدى السماح لطالب البيانات بالوصول إليها.

وأما مفهوم المعالجة الموزعـــة (Distributive Processing) فـــهو يشترك إلى حد ما مع مفـــهوم آخـــر وهـــو مفـــهوم المعالجـــة التعاونيـــة (Cooperative Processing) في نقطة معينة ، وهي تقديم أجزاء من منطق التطبيق (Application Logic). هذه الأجزاء عند ربطها معًا ثم استخدامها، تستطيع تنفيذ المهمة المطلوبة . والفكرة الأساسية في استخدام هذه التقنية هي أننا نحصل على قوة معالجة مضاعفة عند استخدام أكثر من معالج، ونـــرى في الحياة العملية مثالاً واضحًا عند استخدام شبكات الحاســـبات الشـــخصية حيث يستطيع أي مستفيد تنفيذ عمليات مستقلة باستخدام حاســـبه الشـــخصي ولكنه يستطيع في الوقت نفسه مشاركة المستفيدين الآخريـــن فـــي طابعـــة مرتبطة بالشبكة. ولكن هذين المفهومين يختلفان في نقطة أخـــرى وهـــي أن مصطلح "المعالجة التعاونية" يتضمن علاقة مباشرة بيـــن معـــالجين، بينمـــا "المعالجة الموزعة" تتحدث عن تنظيم هرمي. وعلى كل حال فالمعالجة سواء كانت موزعة أو تعاونية تختلف كثيرًا عن إدارة البيانات الموزعة. فمثلاً نجد أن برنامجًا مثل برنـــامج مايكروســـوفت (النوافـــذ لمجموعـــات العمـــل Windows for Work Groups) يقدم إمكانية التشارك فـــي الملفـــات بيـــن المستفيدين في مجموعة العمل بينما يسمح لهم في الوقت نفسه باســـتخدام أي طابعة مثبتة لدى أي عضو في المجموعة.

وباستخدام مزيج من تقنيتي إدارة البيانات الموزعة والمعالجة الموزعة يمكن إعداد تطبيق يستطيع أن يصل إلى قواعد البيانات البعيدة ، وأن يشارك في البرامج بشفافية (أي دون الحاجة إلى تعديلات في هذه البرامج)، ويستطيع كذلك أن يتعاون مع الحاسبات الشخصية البعيدة بحيث يستطيع التطبيق استخدام أي مرفق من مرافق هذه الحاسبات البعيدة في أداء مهامه كأن يرسل تقريرًا من الرياض ليتم طبعه على طابعة فرع الشركة في جدة أو استخدام منفذ إنترنت في جهاز حاسب موجود في جدة من جانب جهاز آخر في الدمام مثلاً.

٢- المشاكل الأمنية في بيئة العميل / الخادم

واحدة من القضايا التي أثيرت في بدايات عمل نظم "العميل / الخادم" كانت أن مطور التطبيق في هذه البيئة كان عليه أن يجيب على سؤال هام: أين يتم تخزين المعلومات الأمنية التي تحدد صلاحيات استخدام البيانات للعملاء؟ وكان المعتاد بالنسبة للبيئة التي تعتمد الحاسب المركزي كخادم أن يتم الاعتماد بالكامل على الحاسب المركزي (الخادم) في حفظ صلاحيات المستفيدين في جداول والتحقق منها عندما يطلب المستفيد الدخول إلى النظام. في هذه الحالة يفحص نظام التشغيل اسم المستفيد وكلمة السر وصلاحياته، ولذلك كان من الضروري أن يعرف الخادم وبكل دقة حجم الصلاحيات الممنوحة لكل مستفيد وهل تقتصر على قراءة البيان أم تمتد إلى التعديل والإضافة. وبمجرد إجازة المستفيد، بناء على جدول الصلاحيات، فإنه لا تتم متابعته بعد ذلك إلا إذا احتاج إلى الدخول إلى تطبيق آخر.

ولكن ظهرت بعد ذلك ممارسات تجعل من عملية الدخول إلى النظام عملية آلية بإدخال الاسم وكلمة السر إلى البرامج التي تعمل آليًا في ساعة محددة من اليوم لتتصل بالخادم للحصول على معلومات (كاستعادة البريد

الإلكتروني الوارد للمستفيد مثلاً). وهذا في حد ذاته أوجد ثغرة أمنية كبيرة تعني أن الدخول إلى الخادم يمكن أن يتم بدون تواجد الشخص بنفسه. بل يمكن كذلك ــ وهذا هو الأخطر ــ أن يتم الدخول إلى الحاسب الشخصي للمستفيد خلسة (عن طريق شبكة إنترنت مثلاً) واستخدام هذه البرامج الآلية الموجودة على القرص الصلب للدخول إلى قواعد بيانات حساسة تحتاج إلى صلاحيات صاحب الجهاز الذي تم استغلال اسمه وكلمة السر الخاصة به دون أن يدري.

هناك بديلان يمكن أن تتم عملية التأكد من شخصية المستفيد وفقًا لأحدهما. البديل الأول يمكن فيه أن يبدأ البرنامج الخاص بالعميل حواراً مع الخادم باستخدام "سجل مستفيد عام" (Common User Profile) ثم يطلب من المستفيد إدخال اسمه وكلمة السر للتدقيق، وفي حالة نجاح التدقيق يقوم الخادم بتلبية كل أسئلة أو طلبات هذا العميل في حدود الصلاحيات الممنوحة له.

البديل الثاني هو أن يقوم الخادم بنفسه بالاتصال بالعميل من خلال برنامج خاص وهذا يلغي الحاجة إلى استخدام سجل المستفيد العام، ولكنه سوف يحرم تطبيق العميل من بعض المرونة والتحكم التي كانت لديه في الأسلوب الأول. والفائدة الأمنية الرئيسية التي نجنيها من السيناريو الثاني هي أن مسئول أمن النظام سيكون في مقدوره باستمرار أن يحدد من هم العملاء الذين يخدمهم الخادم في لحظة معينة.

ولكن أيًا من هذين الأسلوبين لا يأخذ في الاعتبار حالة العميل المتجول المنفصل عن الشبكة الذي قد يتصل من خلال حاسبه الدفتري بالحاسب الخادم من أي مكان.

٣- تأمين التطبيقات

٣-١- الأمن باستخدام القوائم

بمجرد التحقق من شخصية المستفيد يتم تخزين صلاحياته بالنسبة لمختلف البيانات المخزنة بالخادم (أو الخدم إن تعددت الأجهزة الخادمة)، وإذا كنا نستخدم لغة مثل "فيجوال بيسك" أو أي لغة مشابهة فإننا نعرض في شاشتها الافتتاحية مجموعة من القوائم المنسدلة بحيث تمثل كل قائمة تطبيقاً من التطبيقات المستخدمة في المؤسسة. فالعميل يستطيع الدخول إلى أي قائمة (تطبيق) معروضة على الشاشة الرئيسية فتنسدل القائمة ليختار المستفيد منها أي مهمة إذا سمحت صلاحياته بذلك. فإذا لم تكن للعميل صلاحيات تسمح باستخدام قائمة من القوائم (تطبيق من التطبيقات) فلا تظهر هذه القائمة له أصلاً، أو تظهر بلون باهت لا يمكن المستفيد من استخدامها، وبالتالي لا يمكنه ضمناً تنفيذ أي مهمة من مهام هذا التطبيق. وإذا لم تكن للمستفيد صلاحيات استخدام مهمة من مهام القائمة فلا تظهر له هذه المهمة بالمرة أو تظهر باهتة لا تستجيب له، فأنت تحتاج إلى صلاحية معينة للدخول إلى المبنى ثم صلاحية أخرى لدخول غرفة معينة بالمبنى.

يمكن استخدام الأيقونات بدلاً من القوائم فتظهر شاشة بها مجموعة من الأيقونات التي يضغط عليها المستفيد فيدخل إلى التطبيق حيث يجد مجموعة أخرى من الأيقونات وعادة لا تظهر له إلا الأيقونات التي لديه صلاحية استخدامها.

٣-٢- أين نحتفظ بجداول الصلاحيات؟

يمكن التحقق من الصلاحيات باستخدام خادم رئيسي يحتفظ بجميع الصلاحيات الخاصة بالمستفيدين فيما يخص التطبيقات المتاحة في النظام مما

يعني ضرورة أن يحدث اتصال ما بين العميل وهذا الخادم الرئيسي قبل أن يقوم العميل بأي نشاط.

في حالة استحالة هذا الأمر (الاتصال بين العميل والخادم) أو صعوبة تنفيذه فالحل البديل لذلك يتطلب إيجاد نسخة من قاعدة بيانات الصلاحيات الموجودة على الخادم الرئيسي وتحميل هذه النسخة على أجهزة خادم أخرى أو على أجهزة عميل معينة. فإذا تم نسخ جداول الصلاحيات على أجهزة خادم أخرى فهناك عبء ضخم مطلوب وهو عبء تحديثها المستمر والتأكد من دقة هذه النسخ، ويزداد العبء كلما دخل خادم جديد إلى الخدمة.

ولكن ماذا عن الأمن؟ إن تعدد النسخ يعني ازدياد العبء الأمني الناشئ عن المحافظة على سلامتها وسريتها والتأكد من عدم التلاعب فيها، خاصة عند وضع بعض هذه النسخ على أجهزة تعمل بنظام تشغيل ضعيف من الناحية الأمنية. فمثلاً إذا تم وضع نسخة من الملف الأمني على حاسب شخصي خادم فإن أي برنامج من البرامج المساعدة (Utilities) يمكن من خلاله طباعة أي جزء من القرص الصلب الخاص بالجهاز الخادم مما يمثل تسربًا أمنيًا خطيرًا يؤثر ليس فقط على هذه الشبكة ولكن على جميع الشبكات التي تخدمها هذه الجداول الأمنية أي على المنشأة ككل، ولذلك يجب تشفير الملفات الأمنية لتأمين المعلومات التي تحتويها.

إذا وضعت نسخة كاملة من جداول الصلاحيات على حاسبات العملاء (Clients) فإن فقد أو تسرب معلومات أي واحد منها، كأن يسرق جهاز الحاسب الدفتري من صاحبه، يمكن أن يعرض أمن الشبكة بأكملها للخطر. وعلى العكس من ذلك إذا احتفظ العملاء من أصحاب الحاسبات الدفترية (أو الحضنية) بالمعلومات الخاصة بصلاحياتهم هم فقط دون غيرهم، فصحيح إن ذلك سيجعلهم في غير حاجة للاتصال بحاسب أمني مركزي قبل الدخول إلى النظام، ولكن ذلك سوف يعني أن الحاسب هو حاسب **شخصي** بالفعل، أي إنه لا يصلح للاستخدام إلا من جانب صاحبه لأن الصلاحيات المخزنة به تخص

شخصًا معينًا. وهذا الأمر غير عملي على الإطلاق فأجهزة العميل يتم تبادلها بين الأفراد، فمندوبو المبيعات ــ مثلاً ــ يتبادلون أجهزة الحاسب الدفترية فيما بينهم، وإذا استثنينا مشكلة الحاسبات المحمولة فإن أنسب التوصيات تكون بالاحتفاظ بمعلومات الصلاحيات وكافة المعلومات الأمنية على خادم مركزي أو مجموعة من الأجهزة الخادمة. إذا كان من الضروري نسخ المعلومات الأمنية على أجهزة خادم متعددة فقد يكون من الأفضل للخادم المركزي أن يوزع على الخدم الآخرين (الثانويين) فقط تلك المعلومات الأمنية التي يحتاج إليها الخدم الثانويون للتأكد من شخصية هؤلاء العملاء الذين قد يتصلون بالشبكة من خلال هؤلاء الخدم الثانويين. وضمان التنسيق الآني في توزيع هذه المعلومات الأمنية في غاية الأهمية ويجب أن يتم آليًا.

٣-٣- تحديد الصلاحيات على مستوى الحقل

تحدثنا من قبل عن إمكان تحديد صلاحيات المستفيدين في استخدام التطبيقات المختلفة وكذلك تحديد صلاحياتهم في تنفيذ بعض المهام دون غيرها، ولكن ربما تحتاج بعض التطبيقات ــ مثل تطبيقات المرتبات ــ إلى منح صلاحيات تحديث بعض الحقول إلى أشخاص بعينهم أو عدم إظهار هذه الحقول على الشاشة. ومطور التطبيق لا يستطيع، في جميع الأحوال، أن يتنبأ بتلك الحقول التي قد يريد المستفيد أن يتحكم في صلاحيات الوصول إليها.

يلاحظ أن حذف حقل من الشاشة لا يقتصر فقط على منع بيانات هذا الحقل من الظهور على الشاشة بل سيتم كذلك منع كثير من المعلومات المتعلقة بهذا الحقل مثل: بيانات المساعدة (Help text) وجداول الترميز الخاصة برموز هذا الحقل وغير ذلك من المعلومات.

عند تأمين البيانات على مستوى الحقل يجب الاهتمام بأمور ثلاثة، فيجب أولاً تحديد ما إذا كان المطلوب هو تقييد استخدام هذا الحقل بالنسبة لمستفيد معين خلال جميع مهام التطبيق (عرض - حذف - إضافة - تعديل ...) أو أن المطلوب هو التقييد فقط عند استخدام الحقل من خلال شاشة

معينة. الاعتبار الثاني هو هل يتم تحديد عدد الحقول التي يمكن تأمينها بواسطة المستفيد أم لا؟ الأمر الأخير يتعلق بكيفية خفض عمليات الصيانة لكل برنامج مع المحافظة، في الوقت نفسه، على أقصى مرونة عند تأمين الحقول المحددة بواسطة المستفيد.

أفضل الحلول في حالة البيئة التي تستخدم حاسبات شخصية عميلة هي استخدام أسلوب "التوليد الديناميكي للشاشات" والذي يستخدم تصميم شاشة مبدئي (Default) بحيث يتم تعديله بعد ذلك بحذف كل ما يتعلق بالحقول التي يلزم إخفاؤها (اسم الحقل - النص - المهام التي تتعامل معه) من الشاشة الأولية.

٣-٤- تأمين البيانات على مستوى الحقل

هناك ثلاثة أساليب لتنفيذ تأمين البيانات على مستوى الحقل:

١) استخدام ملف منطقي:

الأسلوب الأول هو استخدام ملف منطقي يحتوي على البيانات المتاحة لبرنامج التطبيق. ولكن هذا الأسلوب يخلق العديد من الأعباء غير الضرورية، وكثيرًا ما يجعل المستفيد تحت رحمة كفاءة مطور التطبيق وقدرته على التنبؤ بالحقول المطلوب تأمينها.

فإذا كانت لدينا شاشة بها أربعة حقول فقط فهذا الأسلوب يتطلب إنشاء ستة عشر ملفًا منطقيًا حتى يمكن بالكامل تغطية كافة احتمالات حماية الحقول (عدم الإخفاء، إخفاء الحقل الأول فقط ، إخفاء الحقل الثاني فقط، إخفاء الحقل الثالث فقط، إخفاء الحقل الرابع فقط، إخفاء الحقلين الأول والثاني، إخفاء الحقلين الأول والثالث، إخفاء الحقلين الأول والرابع، إخفاء الحقلين الثاني والثالث، إخفاء الحقلين الثاني والرابع، إخفاء الحقلين الثالث والرابع، إخفاء الحقول الأول والثاني والثالث، إخفاء الحقول الأول والثاني والرابع، إخفاء الحقول الأول والثالث والرابع، إخفاء الحقول الثاني والثالث والرابع، إخفاء جميع الحقول).

٢) تحميل نسخة من ملفات العرض على الخادم:

الأسلوب الثاني هو إنشاء نسخة من ملفات العرض في إحدى مكتبات نظام التشغيل على الخادم وتعديل هذه الملفات عند تحديد الصلاحيات بحيث يتم عرض الحقول المطلوبة فقط.

هذا الأسلوب لا يغير ملف العرض الأصلي ويستخدم فقط بالنسبة للملفات التي يطلب تعديل الصلاحيات فيها. كما يمتاز هذا الأسلوب بأنه يقع بالكامل خارج سيطرة البرنامج التطبيقي ولذلك فلا يوجد أي عبء صيانة أو تعديل على البرامج، ويمتاز كذلك بمرونته بحيث يمكن تقييد استخدام المزيد من الحقول في المستقبل بناء على رغبة المستفيد. أما الحقول المطلوب تأمينها في مواجهة بعض المستفيدين ويمكن تخزين محتوياتها في قاعدة بيانات مؤقتة حتى تتم إضافتها لباقي الحقول بعد انتهاء المستفيد من تعديل الحقول المسموح له بالاطلاع عليها.

من عيوب هذا الأسلوب أن نسخ ملفات العرض المخزنة على الخادم ربما تعرضت للحذف، الأمر الذي يعرض للخطر البيانات التي كان من المفروض تأمينها.

٣) معالجة الشاشة قبل عرضها:

الأسلوب الثالث هو استقبال بيانات الشاشة التي سوف تعرض على المستفيد قبل وصولها إلى الجهاز العميل (Client)، ومن ثم تعديلها بحيث تعكس الصلاحيات المطلوبة (أي تحذف البيانات المطلوب إخفاؤها قبل عرض الشاشة على جهاز العميل).

من الناحية الفنية يعتبر هذا الأسلوب أفضل بكثير من الأسلوبين الأولين، ولكن البرمجيات سوف تعاني من ضعف في تكامل النظام ذلك لأنها يجب أن تتعامل مع نظام العرض على الشاشة، أي إنها لابد أن تعرف المزيد عن بنية "العميل". ولذلك يلزم استخدام (أداة عرض Screen Painter) فورية لتأمين بعض الحقول على جهاز الحاسب الشخصي العميل في بيئة العميل / الخادم.

٣-٥- تأمين قيم معينة داخل الحقول

في بعض التطبيقات الحساسة قد يكون من الضروري حجب تلك السجلات التي تحتوي على بيانات معينة في أحد الحقول عن مجموعة من المستفيدين؛ فربما تود إحدى الشركات مثلاً حجب نسبة الخصم الممنوحة لبعض العملاء، إذا زادت عن ٢٠%، عن بعض موظفي الشركة. يتطلب ذلك معالجة السجلات التي يتم الحصول عليها من الملف بناء على هوية المستفيد، ولا يمكن تنفيذ ذلك بواسطة المنظورات المستخدمة في نظم قواعد البيانات (انظر الفصل الثاني عشر: أمن قواعد البيانات)، لأن هذا الإخفاء يتطلب معرفة المستفيد صاحب الاستفسار والتصرف على هذا الأساس ، مما سيؤدي إلى إعداد نسخ عديدة من كل منظور مما يخلق من المشاكل أكثر مما يحل.

ربما كانت أفضل وسيلة لتحقيق ذلك هي فحص البيانات المستخلصة من قاعدة البيانات بعد الحصول عليها من الخادم، وأن يكون هذا الفحص وفقًا للملف الأمني الخاص بهذا الحقل ومن ثم اتخاذ القرار وفقًا لنتيجة الفحص. في هذه الحالة يمكن أن يتولى جزء التطبيق الموجود على جهاز العميل إجراء هذا الترشيح (Filtering) ويعرض للمستفيد ما هو مطلوب فقط.

هذا النوع من الأمن (تأمين قيم معينة داخل الحقول) مطلوب كثيرًا للتطبيقات الاقتصادية كما تحتاج إليه البنوك بشدة.

٤- استخدام التطبيقات بواسطة الأجهزة المحمولة

ننتقل الآن إلى كيفية تأمين الأجهزة المحمولة، ونقصد بالأجهزة المحمولة (Portable) تلك الأجهزة المتنقلة من نوع (الحاسب الدفتري Note Book) أو (الحاسب الحضني Laptop) أو أي حاسب شخصي غير

مرتبط بالشبكة التي تحتوي نظام العميل / الخادم. وهذه الأجهزة المحمولة تستخدم كثيرًا من جانب مندوبي المبيعات، كما يستخدمها كذلك بعض المديرين لتقديم بعض العروض في أسفارهم ورحلاتهم الخارجية.

٤-١- المشكلة

تكمن المشكلة في هذه الأجهزة في أن المطلوب من العميل أن يتصل أولاً بالخادم من خلال شبكة الهاتف العمومية وإلا فلن يكون في مقدوره استخدام حاسبه المحمول في تطبيقات العميل / الخادم، وذلك لأن بيانات هذا النوع من التطبيقات من المستبعد أن توجد على الجهاز المحمول.

في هذه الحالة يمكن أن يحتوي الحاسب المحمول على المعلومات الأمنية للمستفيد الذي يستخدم الجهاز (أو المستفيدين إذا تعددوا). هذه المعلومات تشمل الأسماء وكلمات السر والصلاحيات، وهي المعلومات المطلوبة لتمكنهم من الدخول إلى بيانات الخادم، وغني عن القول أن هذا الأمر يشكل خرقا خطيرًا للأمن بالإضافة إلى عبء الصيانة والتعديل المستمرين.

٤-٢- الحل

لحل هذه المشكلة يتم استخدام إجراءين للتدقيق، إجراء تدقيق مستقل يخص الخادم وإجراء تدقيق آخر يخص العميل. وبصفة عامة يجب في البداية، وعند طلب الجهاز العميل استخدام تطبيق من نوع العميل / الخادم، أن يقوم هذا التطبيق بتحديد ما إذا كان المستخدم متصلاً بالخادم أم لا. في حالة اتصال العميل بالخادم يتم استخدام إجراءات التدقيق الخاصة بالخادم، بحيث يطلب الخادم من مستخدم الجهاز المحمول أن يدخل اسمه وكلمة السر الخاصة به. أما إجراء تدقيق العميل فيُستخدم في حالة استخدام الحاسب

المحمول باستقلالية عن الخادم، وفي هذه الحالة يجب أن تكون هناك نسخة من الملف الأمني على جهاز العميل توضح كل القيود والإجراءات الأمنية فيما يتعلق بالتطبيقات وكذلك ما يتعلق بالمهام والملفات المرتبطة بهذه التطبيقات، ويستخدم هذا الملف لتحديد شخصية العميل ومن ثم تحديد صلاحياته.

للحد من التعرض الأمني الناشئ عن نسخ البيانات الأمنية الحساسة على الحاسب المحمول يجب أن يتم تصميم تطبيق العميل / الخادم بحيث يتم تشفير المعلومات عند كتابتها أو تعديلها على الحاسب المحمول، وبذلك نحد من المخاطر الناشئة عن فقد الأجهزة المحمولة.

٤-٣- الوقاية

بهذه المناسبة نود أن نوصي مستخدمي هذه الأجهزة بالحرص عليها، فالذي يحدث في بعض المطارات أن هناك عصابات متخصصة في سرقة الحاسبات المحمولة. وتقوم هذه العصابات بمراقبة المسافرين بقرب سير فحص الأمتعة بالأشعة، وعندما يرى اللصوص شخصًا يحمل حاسبًا محمولاً وقبل دخوله إلى سير فحص الأمتعة يقف اللصان أمام الضحية، وعندما يضع الضحية جهازه المحمول على السير يقوم اللص الذي أمامه مباشرة بإعاقته عن عبور بوابة الفحص والوصول إلى جهازه عند خروج الجهاز على السير، بينما يقوم زميل اللص الذي سبق بالخروج من بوابة الفحص بسرقة الجهاز والاختفاء.

وسرقة الجهاز المحمول لا تؤدي فقط إلى ضياع قيمته المادية، ولكن الأهم هو ما يحتويه من معلومات، والأكثر أهمية هو ما يحتويه من ملفات أمنية.

الفصل الثاني عشر

أمن قواعد البيانات

موضوعات الفصل:

(١) مفهوم قواعد البيانات.

(٢) أنواع قواعد البيانات.

(٣) خطة تأمين البيانات.

(٤) وسائل أمن البيانات في النموذج العلاقي.



يعتبر هذا الفصل امتداداً طبيعيًا لسابقه من حيث إنه يلمس احتياجات المبرمج فيما يخص الأمن ، فنبدأ هذا الفصل بتحديد بعض المفاهيم في مجال قواعد البيانات مثل: ماهيتها والهدف منها ومكوناتها ومستخدميها، وتعريف بعض المصطلحات في هذا المجال. نتحدث بعد ذلك عن أنواع قواعد البيانات الهرمية والشبكية والعلاقية، ثم نقدم خطة تأمين البيانات.

نختتم الفصل بوسائل أمن البيانات في النموذج العلاقي باعتباره أهم النماذج المذكورة وأكثرها انتشاراً، فنتحدث عن سلامة العناصر وتكاملها، وتحقيق السلامة المرجعية، وأسلوب حجز البيانات، واستخدام المنظورات في تأمين البيانات، وتوزيع الصلاحيات لاستخدام قاعدة البيانات، ثم استخدام لغة التحكم في البيانات، وفي النهاية نبين دور البرامج المساعدة في أمن البيانات.

١- مفهوم قواعد البيانات

١-١ ما هي قواعد البيانات؟

قاعدة البيانات هي مجموعة متكاملة من البيانات التي تم تنظيمها على الصورة التي تمكن العديد من المستفيدين في المؤسسة من التعامل معها. وحتى يتمكن المستفيدون من التعامل مع قاعدة البيانات بسهولة فإنهم يستخدمون لغات للاستفسار والمعالجة مثل لغة (SQL) ، وحتى يتمكن المتخصصون من إدارة ومعالجة قاعدة البيانات وتأمينها فإنهم يستخدمون نظم إدارة قواعد البيانات (DBMS).

١-٢ لماذا قواعد البيانات؟

في قواعد البيانات يتم تجميع الكثير من بيانات المؤسسة في قاعدة بيانات واحدة أو أكثر، مما يحد إلى درجة كبيرة من تكرار البيانات في ملفات متعددة كما كان الحال قبل قواعد البيانات، ويعفي ذلك من المشكلات

التي كانت تنجم نتيجة تحديث بعض الملفات وعدم تحديث بعضها الآخر.

يتشارك المستفيدون في المؤسسة في نفس البيانات التي تهم أكثر من مستفيد بدلاً من استقلال كل مستفيد بملفاته، فيستفيد مستخدمو البيانات بالتعديلات والإضافات التي يجريها المستخدمون الآخرون مما يؤدي إلى تكامل البيانات ويضمن عدم تعارضها.

إلى جانب ذلك فإن وجود المعلومات في وعاء واحد يسهل فرض ضوابط التحكم في البيانات وتأمينها وهذا هو ما يهمنا الآن.

١-٣ مم تتكون قواعد البيانات؟

تضم قواعد البيانات واحدًا من أهم موارد المؤسسة، ألا وهو مورد المعلومات فتسهل تنظيم استخدامه، ولكي يمكن الاحتفاظ بهذه المعلومات ومعالجتها إلكترونيًا لابد من وجود العتاد اللازم (H/W) كجهاز الحاسب وما يتصل به من أجهزة للتخزين المباشر ووسائط للنسخ الاحتياطي، ولابد كذلك من توافر البرمجيات اللازمة (S/W) كنظام لإدارة قواعد البيانات (DBMS) إلى جانب بعض البرمجيات الأخرى المرافقة التي تساعد على التحكم في المعلومات وتنظيمها واسترجاعها وعرضها على المستفيد في الصورة التي يريدها.

١-٤ من هم الذين يستخدمون قاعدة البيانات؟

الكثير من المستفيدين ومن المتخصصين يستخدمون قاعدة البيانات ولكن لكل منهم دور يختلف عن الآخرين:

١) المستفيدون (Users):

وهؤلاء إما أن يكونوا من موظفي الإدارات المستفيدة المسئولين عن إدخال البيانات وتحديثها، أو أن يكونوا من طبقة الإدارة العليا أو مديري الإدارات المستفيدة الذين يستخدمون هذه البيانات بالاستفسار عنها أو استخدام

البرامج المعدة سلفًا لاستخراج المعلومات والتقارير المطلوبة من قاعدة البيانات.

٢) المبرمجون (Programmers):

وهي الفئة من المتخصصين التي تتولى إعداد البرامج التي تخرج التقارير التي تحتاج إليها الإدارة العليا والبرامج التي تتولى تنظيم البيانات ومعالجتها.

٣) مدير النظام (Systems Administrator)

ومدير قاعدة البيانات (Database Administrator):

وهي الفئة من المتخصصين التي تتولى العناية بهياكل البيانات والمسئولة عن إعداد الإجراءات اللازمة لتأمين البيانات ولاستعادتها في حالة فقدها.

٤) مسئول أمن قاعدة البيانات (DB security administrator):

وهو المسئول النهائي عن أمن البيانات وتأمين النسخ الاحتياطية واسترجاع البيانات في حالة فقدها وإعادة قاعدة البيانات إلى الحالة المطلوبة. وهو المسئول عن وضع خطة تأمين البيانات وعن توزيع الصلاحيات ومراقبة استخدام قاعدة البيانات والتأكد من عدم وجود مخالفات أمنية.

٥) المشغلون (Operators):

هي الفئة من المتخصصين التي ربما لا تتعامل بصفة مباشرة مع قاعدة البيانات إلا أنهم المسئولون عن تنفيذ الإجراءات المعدة من جانب مسئول الأمن ومدير النظام ومدير قاعدة البيانات، وهم المسئولون عن تنظيم وحفظ واستعادة الأشرطة التي تحتوي على سجل النظام وعلى النسخ

الاحتياطية، وهم مسئولون كذلك عن تشغيل النظام وإيقافه ومتابعة الرسائل التي يخرجها النظام.

١-٥ تعريفات

نورد هنا بعض التعريفات التي قد يكون من الضروري الاتفاق عليها عند تناول موضوع قواعد البيانات:

١) قاعدة البيانات (Data base):
هي مجموعة متكاملة من البيانات تم تنظيمها على الصورة التي تمكن العديد من المستفيدين بالمؤسسة من التعامل معها.

٢) العنصر (Entity):
هو شيء أو حدث تحتفظ المؤسسة عنه ببيانات، مثل: الموظف أو الدورة التدريبية التي يحصل عليها الموظف أو طلب بضاعة مقدم من العميل.

٣) خواص العنصر (Entity attributes):
هي صفات يتصف بها العنصر بحيث تميزه عن باقي العناصر المشابهة ، ففي مثال الموظف يعتبر اسم الموظف خاصة من خواص عنصر الموظف، والإدارة التي يعمل بها هي أيضًا خاصة، وفي حالة الأصناف المطلوبة من المخزن فإن رقم الصنف المطلوب من المخزن هو خاصة من خواص عنصر طلب البضاعة وهو أيضًا خاصة من خواص عنصر الصنف.

٤) **العامود (Column):**

هو الوحدة الأساسية للجدول أو هو خاصة من خواص العنصر.

٥) **الصف (Row):**

هو مجموعة من القيم المفردة لأعمدة الجدول، فلكل عامود في الجدول توجد قيمة معينة ويضم الصف هذه القيم جميعها وهو ما يقابل السجل في الملفات.

٦) **السجل (Record):**

هو ما يمثله الصف في جدول البيانات، فبالنسبة لجدول الموظفين يكون لكل موظف سجل (أي صف).

٧) **الجدول (Table):**

يتكون الجدول من مجموعة محددة من الأعمدة وعدد غير محدد من الصفوف غير المرتبة، وهو يستخدم لتمثيل عنصر معين.

٨) **قيمة ملغاة (Null):**

للتعبير عن أنه لا توجد قيمة لهذا العامود في هذا الصف.

٩) **المفتاح (Key):**

هو عنصر بيانات أو هو حقل ضمن السجل (الصف) يستخدم لتمييز هذا السجل، وهو إما أن يكون مفتاحًا أوليًا (Primary key) يميز السجل تمامًا عن غيره من السجلات بحيث يكون هذا السجل متفردًا (Unique) أو يكون مفتاحًا ثانويًا (Secondary key) وهو في هذه الحالة يميز السجل أيضًا ولكنه لا يجعله متفردًا.

١٠)سجل الوقائع (Log):

يحتوي على مجموعة من السجلات التي يسجل كل منها واقعة من وقائع التعديل أو الإضافة أو الحذف للبيانات ويمكن الرجوع إليه عند فقد بعض هذه الوقائع لاستعادة قاعدة البيانات في وضعها الصحيح.

١١) استعادة الوضع (Recovery):

عملية إعادة بناء قاعدة البيانات بعد حدوث انهيار للنظام أو تلف قاعدة البيانات.

١٢) حجز البيانات (Locking):

الأسلوب المتبع للتأكد من تسلسل الأحداث التي تؤثر على البيانات لضمان سلامتها وتكاملها، عن طريق منع المستفيدين من استخدام أو تعديل البيانات التي يجرى تعديلها حتى يتم الانتهاء من ذلك.

١٣) لغة الاستفسار (SQL):

هي لغة (Structured Query Language) وتستخدم للاستفسار عن البيانات ولإنشاء موارد قاعدة البيانات، مثل الجداول، وتعديل هذه الموارد، كما تستخدم لتنظيم استخدام هذه الموارد.

٢- أنواع قواعد البيانات

تطورت نظم قواعد البيانات على مدى العقود الثلاثة الأخيرة بناءً على تطور نماذج البيانات المستخدمة، وهناك ثلاثة نماذج شهيرة لها: هي النموذج الهرمي (Hierarchical) والنموذج الشبكي (Network) ثم آخر وأهم هذه النماذج وهو النموذج العلاقي (Relational) وهو ما سنركز عليه فيما يلي:

٢-١ قواعد البيانات الهرمية(Hierarchical databases)

وهو النوع المناسب للبيانات التي تتفق طبيعتها والطبيعة الهرمية حيث تكون العلاقة بين البيانات هي إما علاقة مفردة (١:١)، أو علاقــة متعــددة (١:ن) مثل طلبات العملاء من الشركة حيث يكون للعميل الواحد طلب واحـد أو أكثر، ولكن هذه الطلبات ليست لها أي علاقة بعميل آخر فلا ينتمي الطلب الواحد إلا إلى عميل واحد.

ويعيب هذا الأسلوب تكرار البيانات والبطء الذي يميز الاستفســارات التي لا تتفق طبيعتها والطبيعة الهرمية لهذا النموذج.

ولعل أشهر نظم إدارة قواعد البيانات التي تتبع هذا النموذج هو نظــام (IMS) من شركة (آي. بي.إم .I.B.M).

٢-٢ قواعد البيانات الشبكية (Network databases)

وهو النوع المناسب للبيانات التي تتشابك فيها العلاقات بين العناصر، ففي هذا الأسلوب يتم تمثيل البيانات كمجموعات من الســجلات والعلاقــات المختلفة بين هذه السجلات مثل طلبات العملاء عندما تتــم ترجمتــها إلــى منتجات محددة مطلوبة من المخازن، فكل منتج يتم طلبه من المخـــزن قــد يكون مطلوبًا من أكثر من عميل، والعميل الواحد قد يطلب أكثر من منتـــج، وهذه الشبكة من العلاقات هي التي شجعت على ظهور هذا النموذج الشبكي.

يعيب هذا النموذج التعقيد وصعوبة الاستخدام، كما أنــه قـد صمـم ليناسب لغات الجيل الثالث من حيث إنها تتعامل مع السجلات واحدًا واحـدًا وبذلك فهو يفتقر إلى مزية الاستفادة من إمكانات لغات الجيل الرابع التي فـي مقدورها التعامل مع مجموعة من السجلات من خلال أمر واحد.

ومن أشهر أنواع نموذج (كوداسيل CODASYL) الشبكي وأكثرهـــا انتشاراً هو نظام (IDMS).

٢-٣ قواعد البيانات "العلاقية"(Relational databases)

هذا النوع الأخير الذي اعتمد في تصميمه على النمـــــوذج "العلاقـــي" لتوصيف البيانات (Relational Data Model) يعتبر أشهر الأنواع الثلاثـــة وأفضلها لأسباب عديدة، منها أن البيانات في هذا النوع يتم تنظيمـــها علـــى شكل جداول حيث يمثل كل جدول أحد العناصر (Entities) في المؤسســـة، مثل الموظف فهو عنصر، أو الـــدورات التدريبيـــة التـــي يحصـــل عليـــها الموظفون فهي كذلك عنصر ، وهكذا ... . وصورة الجدول هي أبسط صور تنظيم البيانات وأكثرها منطقية وأقربها إلى الفهم. فإذا أردنا توصيف بيانـــات موظفي المؤسسة فأنسب الأشكال لذلك هو شكل الجدول حيـــث يمثـــل كـــل موظف في المؤسسة بصف في هذا الجدول، بينما تمثل أعمدة الجدول بيانات الموظفين، فهناك عامود للاسم، وعامود للراتب الأساسي، وهكذا... .

ويمكن إيجاد علاقة بين عدة جداول للربط بينها، وفي هذه الحالة يمكن تطبيق قواعد الجبر العلاقي (Relational algebra) بين هذه الجداول.

وهذا الأسلوب يناسب معظم أنواع البيانات مما أضفى عليه الجاذبيـــة التي يتمتع بها، ومن مزاياه كذلك أنه يناسب لغات البرمجة الحديثة ويمكـــن الاستفسار عن البيانات فيه باستخدام لغة الاستفسار الشهيرة (SQL).

وأشهر هذه الأنواع نظام قواعد البيانات (DB2) ونظام "أوراكل".

٣- خطة تأمين البيانات

٣-١ الهدف من الخطة

المقصود بتأمين قواعد البيانات هو حماية البيانات من الفقد أو التلـــف أو سوء الاستخدام، ثم تأمين استعادة هذه البيانات إذا فشلت إجراءات تأمينـــها

لسبب أو لآخر. أي أننا نتحدث عن شق الوقاية وشق العـــلاج معًـــا. ومـــن الواضح أن هذا يحتاج إلى إعداد جيد وتخطيط مسبق وهذا ما نعني به وضع خطة تأمين البيانات.

ومن المناسب هنا أن نؤكد -على عكس ما قد يظنه بعـــض موظفـــي الحاسب- أن توزيع الصلاحيات بين المستفيدين لا يجب أن يكون هو الشغل الشاغل لمسئول أمن قاعدة البيانات، فالأكثر أهمية هـــو ســـلامة البيانـــات وتكاملها والاحتفاظ بنسخ احتياطية لها، وإعداد إجراءات مسبقة يتم تنفيذهـــا عند فقد البيانات، وفي النهاية تأتي مسألة الصلاحيات لتنظيم تداول البيانـــات بين مستخدميها.

٣-٢- تحديد الموارد المطلوب حمايتها

يجب عند وضع خطة تأمين البيانات تحديد الموارد المطلوب حمايتـــها وتختلف هذه الموارد من نظام إدارة قواعد بيانات إلى آخر ومن هذه الموارد التي يجب أن يضعها المخطط لأمن البيانات في اعتباره:

١) **البيانات نفسها التي تحتويها الجداول.**

٢) **هياكل البيانات .**

٣) **البرامج التي تعالج البيانات.**

٤) **إجراءات نسخ البيانات واستعادتها.**

٥) **الوسائط التي تحتوي على البيانات مثل الأقراص الممغنطة.**

٦) **تنفيذ البرامج والإجراءات.**

٧) **الطرفيات.**

٣-٣- وضع خطة تأمين البيانات

خطة تأمين البيانات نحدد فيها أساليب التأمين المناسبة لبيئة قواعد البيانات الخاصة بالمؤسسة لتحقيق كل مما يأتي، ويجب أن نبين أيها يتم تحقيقه آليًا بواسطة نظام إدارة قواعد البيانات نفسه وأيها يلزم اتخاذ إجراءات أخرى لتحقيقه :

١) سلامة العناصر وتكاملها وكيف يمكن ضمان ذلك.

٢) السلامة المرجعية وكيفية ضمان تحقيقها.

٣) أسلوب حجز البيانات عند استخدامها.

٤) المنظورات المناسبة للقطاعات العريضة من المستخدمين.

٥) هيكل الصلاحيات للمتعاملين مع قاعدة البيانات بالنسبة للموارد المختلفة.

٦) كيفية توزيع الصلاحيات باستخدام لغة التحكم في البيانات المستخدمة في المؤسسة.

٧) حصر البرامج المساعدة اللازمة لتأمين البيانات وتحديد دوريات تنفيذها.

وسنحاول التركيز، عند التعرض لهذا الموضوع، على النموذج العلاقي نظرًا لانتشاره.

٤- وسائل أمن البيانات في النموذج العلاقي

يتيح نموذج البيانات العلاقي عدة وسائل تحقق ضمان تأمين سلامة البيانات وتكاملها (Securing Data Integrity)، ولا تخلو جميع نظم إدارة قواعد البيانات العلاقية الحديثة من هذه الوسائل وهي:

٤-١- سلامة العناصر وتكاملها (Entity Integrity)

تتحقق سلامة العناصر وتكاملها عن طريق تأمين **المفتاح الرئيسي للجدول** وضمان صحته، فتشترط أن يكون المفتاح الرئيسي للجدول **متفردًا غير متكرر (Unique)** فلا يكون لصفين في الجدول نفس المفتاح، كما تشترط أن تكون هناك **قيمة محددة للمفتاح الرئيسي** للجدول أي لا يُترك مكانه خاليًا في أي صف من صفوف الجدول (NOT NULL) .

٤-٢- السلامة المرجعية (Referential Integrity)

يعتبر هذا المبدأ من أهم المبادئ التي تضمن صحة البيانات وتؤمِّن سلامتها وتكاملها، ويضع هذا المبدأ شرطًا مهمًا في حالة اعتماد جدول ما على جدول آخر (أي حين تعتمد قيم أحد أعمدة هذا الجدول -ويطلق على هذا العامود اسم المفتاح الخارجي (Foreign key) - على المفتاح الرئيسي لجدول آخر). وهذا الشرط هو أن تكون القيم الواردة في هذا العامود في الجدول المشير (Referring table) (أي الجدول الذي يعتمد على الجدول الآخر) مساوية لأحد قيم المفتاح الرئيسي في الجدول المشار إليه (Referenced table) .

وحتى يمكن المحافظة على السلامة المرجعية في النموذج العلاقي يتم تطبيق قواعد معينة عند إضافة السجلات (الصفوف) أو حذفها من الجداول، وهذه القواعد هي:

٤-٢-١- قاعدة الإضافة

هذه القاعدة تضع شرطًا يتم تطبيقه عند إضافة أي صف جديد إلى **الجدول المشير (Referring table)** وهو:

"عند إضافة صف جديد للجدول المشير (وهو ذلك الجدول الذي يعتمد على جدول آخر) يتم اختبار المفتاح الخارجي (foreign key) في هذا الصف {وهو العامود الذي يشير إلى المفتاح الرئيسي (primary key) في الجدول الآخر المشار إليه (Referenced table) } وذلك للتأكد من أن هذا **المفتاح الخارجي يأخذ قيمة مساوية لأحد قيم المفتاح الرئيسي للجدول المشار إليه** {أو أن يكون بلا قيمة (NULL) إذا كان مسموحًا بذلك}.

٤-٢-٢- قاعدة الحذف

هذه القاعدة تضع شرطًا يلزم تحقيقه عند حذف الصفوف من الجدول المشار إليه (Referenced table) وهو :

"عند محاولة حذف صف من الجدول المشار إليه بينما كان هناك أحد الصفوف في الجدول المشير يعتمد على هذا الصف المطلوب حذفه ، أي كان المفتاح الخارجي بأحد صفوف الجدول المشير يأخذ قيمة المفتاح الرئيسي للصف المطلوب حذفه من الجدول المشار إليه، فإن هناك ثلاثة بدائل للأسلوب الذي يتصرف به النظام، ويجب أن يتم تحديد البديل المطلوب مسبقًا":

١) **عدم الحذف (RESTRICT):**

لا يسمح النظام بحذف هذا الصف من الجدول المشار إليه.

٢) **حذف جميع الصفوف التابعة (CASCADE):**

يسمح النظام بحذف هذا الصف من الجدول المشار إليه على أن يتم حذف جميع صفوف الجدول المشير التي تأخذ مفاتيحها الخارجية قيمة المفتاح الرئيسي لهذا الصف المحذوف.

٣) **إلغاء قيمة المفتاح الخارجي (SET NULL):**
يسمح النظام بحذف هذا الصف من الجدول المشار إليه على أن تلغى قيم المفاتيح الخارجية المعتمدة عليه بأن يوضع مكانها في الجدول المشير القيمة (NULL).

٤-٣- حجز البيانات (Locking)

أحد الإجراءات المهمة لتأمين البيانات في قواعد البيانات هو أسلوب حجز البيانات التي يجرى تعديلها بواسطة أحد المستفيدين حتى يتم هذا التعديل ثم تتاح البيانات بعد ذلك لأي مستفيد آخر.

وهذا الحجز قد يكون **حجزًا محدودًا** (Shared lock) بحيث يسمح للمستفيدين الآخرين بقراءة البيانات دون تعديلها، وقد يكون **حجزًا مطلقًا** (Exclusive lock) لا يسمح لأي مستفيد باستخدام البيانات لا بالقراءة ولا بالتعديل.

٤-٤- المنظورات (Views)

يستخدم أسلوب المنظور (View) في قواعد البيانات العلاقية كوسيلة ممتازة لتأمين البيانات (إلى جانب فوائده الأخرى). وفي هذا الأسلوب يتم تحديد (نافذة) للمستفيد يرى منها ما يهمه فقط من قاعدة البيانات، فبعض المستفيدين لا يهمه من الجدول كل أعمدته أو كل صفوفه، ولذلك يتم تحديد عدد محدد من الأعمدة ومن الصفوف لهذا المستفيد فلا يرى من الجدول سواها.

فإذا أخذنا مثالاً على ذلك جدول بيانات الموظف في المؤسسة فيمكن تحديد أعمدة معينة تهم إدارة شئون الموظفين وأعمدة أخرى تهم الإدارة المالية، وهكذا ... وفي هذه الحالة لا يرى الموظفون التابعون لكل إدارة إلا الأعمدة التي تم تحديدها في المنظور الخاص بإدارتهم.

اسم الموظف	الراتب الأساسي	الإدارة التابع لها	تاريخ الميلاد	المؤهل الدراسي	عدد الأولاد
		إدارة الحاسب			
		الإدارة المالية			
		إدارة المشروعات			
		إدارة الحاسب			
		إدارة المشروعات			

	هذه الصفوف تتبع المنظور الخاص بإدارة المشروعات
	هذه الصفوف تتبع المنظور الخاص بالإدارة المالية
	هذه الصفوف تتبع المنظور الخاص بإدارة الحاسب

الشكل (١٢-١) استخدام المنظورات لتأمين صفوف الجدول

وفي نفس المثال ربما كان من المناسب أن تقصر كل إدارة اهتمامها على موظفيها وحدهم دون غيرهم ، وفي هذه الحالة يقتصر المنظور الخاص بكل إدارة على الصفوف الخاصة بموظفي هذه الإدارة فقط، ويمثل الشكل (١٢-١) جدول الموظفين ويظهر فيه المنظور الخاص بإدارة الحاسب ويضم الصفوف الخاصة بموظفي هذه الإدارة والمنظور الخاص بإدارة المشروعات ويضم موظفيها.

ويبين الشكل (١٢-٢) كيف يشتمل المنظور على عدد من الأعمدة فالمنظور الخاص بإدارة شئون الموظفين يتكون من الأعمدة التي تهم هذه الإدارة بينما يتكون المنظور الخاص بإدارة الشئون المالية من الأعمدة التي تهم هذه الإدارة ومن الطبيعي أن تكون بعض الأعمدة مشتركة بين المنظورين.

كما يمكن للمنظور أن يضم عدداً محدداً من الأعمدة وعدداً محدداً من الصفوف أيضاً.

اسم الموظف	الراتب الأساسي	الإدارة التابع لها	تاريخ الميلاد	المؤهل الدراسي	عدد الأولاد

(تظليل رأسي)	هذه الأعمدة تتبع المنظور الخاص بإدارة شئون الموظفين
(تظليل أفقي)	هذه الأعمدة تتبع المنظور الخاص بإدارة الشئون المالية
(تظليل شبكي)	هذه الأعمدة مشتركة وتتبع المنظور الخاص بكل من الإدارتين

الشكل (١٢-٢) استخدام المنظورات لتأمين أعمدة الجدول

٤-٥- الصلاحيات (Authorities)

تأتي عملية توزيع الصلاحيات على المستفيدين لتنظيم تداول البيانات واستخدامها وتنظيم من الذي يحق له الاطلاع على أي المنظورات ومن الذي من واجبه تعديل أي الجداول ومتى يتم ذلك ومن أي الطرفيات بالذات يجب أن يتم ذلك، وهكذا ... ويحفظ نظام إدارة قواعد البيانات هذه الصلاحيات إما في قاموس البيانات أو في جداول النظام وفقًا لنظام إدارة قواعد البيانات المستخدم بحيث يرجع إليها النظام عند أي طلب لاستخدام البيانات من جانب المستفيدين. وتتباين النظم المختلفة فيما بينها في طريقة تحديد هيكل الصلاحيات وفي أسلوب منح هذه الصلاحيات أو حجبها.

يعمل نظام إدارة قواعد البيانات جنبًا إلى جنب مع نظام الاتصال المباشر (Online) مثل: نظام (CICS) أو نظام (TSO) أو (COMPLETE)، وجنبًا إلى جنب مع نظام التشغيل نفسه (MVS) أو (VM) أو (VMS) أو غيرهم، وجنبًا إلى جنب مع نظام أمن البيانات المستخدم مثل: (RACF) أو (ACF/2) أو (TOPSECRET) أو غيرهم، ولذلك يجب أن تتعايش إجراءات الصلاحيات بين هذه النظم جميعها، فلكل منها نظام الصلاحيات الخاص به، ويجب لهذه الإجراءات ألا تتعارض ولا تتصادم ولا تتكرر ولا تتعدد حتى لا تعرقل العمل أو تقلل من كفاءته، وفي نفس الوقت يجب لهذه الإجراءات أن تتناغم بحيث لا تترك ثغرة تهدد أمن البيانات، بل يجب أن يتم التخطيط المسبق لها وتنظيمها، وعادة تكون هذه المهمة من مهام مسئول أمن المعلومات الذي يجب أن يتبع مدير مركز المعلومات مباشرة وألا يكون ضمن موظفي أي إدارة من إدارات المركز حتى يمكنه أداء مهمته التنظيمية والرقابية بحرية.

ولكي يتم تحقيق ما ذكرناه من ضرورة التناغم وعدم التصادم أو التكرار لابد أن يكون لكل مستفيد رقم استخدام واحد ينفذ بواسطته إلى

البيانات من أي نظام اتصال مباشر ولا يستخدم في النظام سوى هذا الرقم لذلك المستخدم، وتتحدد لهذا الرقم الصلاحيات المناسبة في كل مراحل التعامل مع البيانات بحيث تقل بقدر الإمكان نقاط التفتيش مع الضمان الكامل لأمن البيانات.

ويجب عند وضع خطة تأمين البيانات تحديد الصلاحيات لكل مجموعة من مجموعات المستفيدين الذين يمكن تصنيفهم على النحو التالي:

٤-٥-١- المستفيدون

١) الإدارة العليا.
٢) مديرو الإدارات.
٣) الموظفون المسئولون عن إدخال البيانات وتحديثها.
٤) الموظفون الذين يستخدمون البيانات.
٥) جمهور المتعاملين مع المؤسسة.

٤-٥-٢- متخصصو الحاسب الآلي

١) مدير النظام.
٢) مدير قاعدة البيانات.
٣) مدير أمن النظام.
٤) المبرمجون.
٥) المشغلون.

٤-٦- لغة التحكم في البيانات (DCL)

في نظم الأمن التي تنظم استخدام قواعد البيانات يتم تحديد الموارد المطلوب حمايتها والصلاحيات التي تمنح للمستفيدين للوصول إلى بياناتهم ويتم ذلك من خلال **لغة التحكم في البيانات (Data Control Language)**

أو (DCL). وتعتمد هذه اللغة على أمرين أساسيين وفقًا للغة القياسية (لغة الاستفسار البنائية SQL).

٤-٦-١ أمر منح الصلاحية (GRANT)

ويستخدم لمنح الصلاحية لمستفيد معين أو مجموعة من المستفيدين لاستخدام جدول معين أو منظور معين أو تنفيذ برنامج معين أو استفسار معين. كما يستخدم هذا الأمر لنقل صلاحيات مستفيد ما إلى مستفيد آخر (ليحل محله في حالة غيابه مثلاً) .

٤-٦-٢ أمر حجب الصلاحية (REVOKE)

ويستخدم لحجب الصلاحية التي سبق منحها لمستفيد معين أو مجموعة من المستفيدين سواء بالكامل أو حجبها جزئيًا بالنسبة لجزء معين من البيانات أو البرامج، ويستخدم هذا الأمر لحجب جميع الصلاحيات التي منحت بواسطة شخص معين.

٤-٧ البرامج المساعدة (Utilities)

تستخدم البرامج المساعدة في تأمين البيانات والحفاظ عليها وتقوم في هذا المجال بدور كبير، إذ تقوم هذه البرامج بالوظائف التالية لضمان أمن وسلامة البيانات:

١) تحميل جداول البيانات أو إعادة تنظيمها.
٢) فحص فهارس الجداول للتأكد من توافقها مع البيانات الموجودة في الجداول والتأكد من توافر شروط السلامة المرجعية في البيانات.
٣) أخذ النسخ الاحتياطية للبيانات وتحميلها على أشرطة.
٤) استعادة البيانات من النسخ الاحتياطية أو استخدام سجل وقائع النظام (Log) لاستعادتها أو من الاثنين معًا.

الفصل الثالث عشر

أمن شبكات نقل المعلومات

موضوعات الفصل:

(١) مفهوم الشبكات وأنواعها.

(٢) الأجهزة المكونة للشبكات.

(٣) برامج تشغيل الشبكات ومراقبتها.

(٤) الأساليب الحديثة لنقل البيانات.

(٥) مصادر تهديد البيانات خلال مرورها بالشبكات.

(٦) ضمان صحة البيانات المرسلة.



نتناول في هذا الفصل موضوع أمن شبكات نقل المعلومات، بل يمتد تناولنا لهذا الموضوع عبر الفصلين القادمين أيضًا من خلال تناولنا لأمن شبكات "إنترانت" المحلية وشبكة "إنترنت" العالمية.

نبدأ الفصل بمقدمة عن مفهوم الشبكات واستخداماتها وأنواعها، ثم نتناول الأجهزة المكونة للشبكات وشرح استخدام هذه الأجهزة، ثم يأتي دور الحديث عن البرامج، فنناقش دور برامج تشغيل الشبكات، وبرامج مراقبة أداء الشبكات في المحافظة على الأمن. ونقدم بعد ذلك بعض الأساليب الحديثة لنقل البيانات، ثم نحدد مصادر تهديد البيانات خلال مرورها بالشبكات، وأمثلة على ذلك، ونقدم في شكل جدول الأخطار التي تهدد الشبكات والأثر الذي يحدثه كل خطر في حال حدوثه، وكيفية مواجهة هذا الخطر. ونختتم الفصل بالإجراءات الواجب اتباعها لضمان صحة البيانات المارة عبر الشبكة.

١- مفهوم الشبكات وأنواعها

١-١- شبكات نقل البيانات

عندما نتكلم عن "**شبكات الحاسب**"، أو عن "**شبكات نقل البيانات**" (**Data Networks**) فإننا نعني الوسيلة التي يمكن عن طريقها لمجموعة من أجهزة الحاسب أن تتصل معًا وأن تتبادل البيانات فيما بينها. ويتم ذلك عن طريق أجهزة اتصال خاصة مرتبطة بخطوط اتصال. وتستخدم في نقل البيانات إجراءاتٌ متفق عليها (**بروتوكولات**) ، وتتأثر كفاءة أداء الشبكة بنوع **خطوط الاتصال المستخدمة**، كما يؤثر اختيار "**طبوغرافية الشبكة**" (**Topology**) في تكلفة إنشاء الشبكة وفي مدى مرونة التوسع المستقبلي.

١-٢- لماذا نستخدم الشبكات؟

يمكن تلخيص أهمية الشبكات ولماذا نستخدمها في النقاط التالية:

(١) تمكين المستفيدين من **التشارك في الموارد**، فيمكن بذلك **تفادي تكرار الموارد مرتفعة الثمن** كطابعات الليزر الملونة أو الراسمات المتقدمة أو الكاميرات الرقمية أو غير ذلك، كما يمكن **التشارك في التطبيقات والبرامج** بين العديد من المستفيدين مما يخفض التكلفة، وفي الوقت نفسه يسهل عملية تحديث البرمجيات إلى نسخٍ أحدث وذلك بتركيب نسخةٍ واحدةٍ فقط يستخدمها الجميع.

(٢) تقليل الآثار المترتبة على الأعطال وذلك لتعدد بدائل معالجة البيانات، ففي حالة تعطل بعض الخطوط تستمر الخدمة نتيجة تعدد المسارات البديلة لنقل البيانات.

(٣) في حالة إضافة عناصر جديدة للشبكة، سواء كانت طابعات أو نهايات طرفية جديدة فإن هذه العناصر الجديدة تدخل إلى الخدمة فوراً.

(٤) تحقيق زمن استجابةٍ أفضل، ففي حالة الشبكات المحلية تكون سرعة نقل البيانات عبر الكوابل أكبر من سرعة الحاسب الشخصي نفسه. وفي الشبكات التي تربط الحاسبات الكبيرة يمكن تنفيذ المعالجة المتوازية (Parallel processing) مما يرفع من كفاءة الأداء بشكل كبير.

(٥) يمكن خفض الزمن المنقضي والموارد المستخدمة في عمليات النسخ الاحتياطية حيث تتم هذه العملية مرة واحدة بواسطة مسئول الشبكة نيابةً عن كل المستفيدين.

١-٣- أنواع الشبكات

يمكن تصنيف الشبكات، بصفةٍ أساسية، إلى ثلاثة أنواع طبقًا للمساحة الجغرافية التي تغطيها الشبكة:

(١) الشبكات المحلية (Local Area Networks):

ويطلق عليها LANs ، وهي شبكة اتصال للحاسبات تغطي منطقة جغرافية محددة لا تزيد عادة عن بضعة كيلومترات مربعة، وغالبًا ما تكون أقل من ذلك بكثير. وفي هذا النوع من الشبكات يتم نقل البيانات بسرعة كبيرة نسبيًا قد تصل إلى عشرات أو مئات الميجا بايت في الثانية في نطاق المؤسسة أو معمل الحاسبات أو حرم الجامعة، وعادة تضم الشبكة مجموعة من الحاسبات الشخصية مرتبطة معًا.

(٢) شبكات المناطق (Metropolitan Area Network):

ويطلق عليها (MANs) ، وهي شبكة اتصال للحاسبات تغطي منطقةً أوسع، وفي العادة تكون مجموعةً من الشبكات لا شبكة واحدة. وهذه الشبكة عالية السرعة (حوالي ٨٠ ميجا بايت في الثانية). وهي قادرة على إرسال الصورة والبيانات عبر مدى يتراوح من ٤٠ إلى ٨٠ كيلومترًا. وباستخدام أسلوب (FDDI) يمكن إنشاء شبكة من هذا النوع تغطي منطقةً معينةً مثل منطقة وسط المدينة، بحيث تشترك في هذه الشبكة المكاتب والمتاجر والشركات الصغيرة الموجودة في هذه المنطقة.

(٣) الشبكات الكبيرة (Wide Area Networks):

ويطلق عليها (WANs) ، وهي شبكة تقوم بوصل الحاسبات عبر مناطق قد تصل عمليًا إلى تغطية مساحة الكرة الأرضية بأكملها. وكثيرًا ما تستخدم فيها الأقمار الاصطناعية كوسيلة اتصال أو شبكات الهاتف أو الكابلات البحرية، ومن أشهر هذه الشبكات شبكة إنترنت (Internet) التي تغطي العالم بأجمعه وتتصل بها عدة شبكات أخرى.

٢- الأجهزة المكونة للشبكات

تتكون الشبكة من الناحية المادية (Hardware) من هذه الأنواع من الأجهزة:

٢-١- النهايات الطرفية (Terminals)

ومن خلالها يستطيع المستفيد الدخول إلى الشبكة والاستفادة من خدماتها.

٢-٢- الحاسب الكبير (Host computer)

وعن طريقه يتم تنفيذ عمليات معالجة البيانات مثل: نقل وتوزيع الرسائل والتشغيل عن بعد وغير ذلك.

٢-٣- معالج الاتصالات (Communication processor)

وهو عبارة عن حاسب صغير ينوب عن الحاسب الكبير في بعض الوظائف مثل: تطبيق البروتوكول، واكتشاف الأخطاء وتصحيحها، وغير ذلك.

٢-٤- وسائط نقل البيانات

التي يتم من خلالها ربط الحاسبات المشتركة في الشبكة، ولما كانت الشبكات هي وسيلة اتصال بين الحاسبات فإن وسائط نقل البيانات تعتبر أهم المكونات المادية للشبكة، وهي تتضمن:

٢-٤-١- الكوابل

(١) الزوج المجدول غير المعزول (Unshielded Twisted Pair).

(٢) الزوج المجدول المعزول (Shielded Twisted Pair).

(٣) الكابل المحوري (Coaxial cable).

(٤) كابل الألياف البصرية (Fiber Optic Cable).

٢-٤-٢- شبكة الهاتف

(١) الخطوط الخاصة (Leased Lines).

(٢) الخطوط المؤقتة (Dialup Lines).

٢-٤-٣- الاتصال اللاسلكي

(١) الأشعة تحت الحمراء (Infrared Rays).

(٢) موجات "الميكروويف" (Microwaves) .

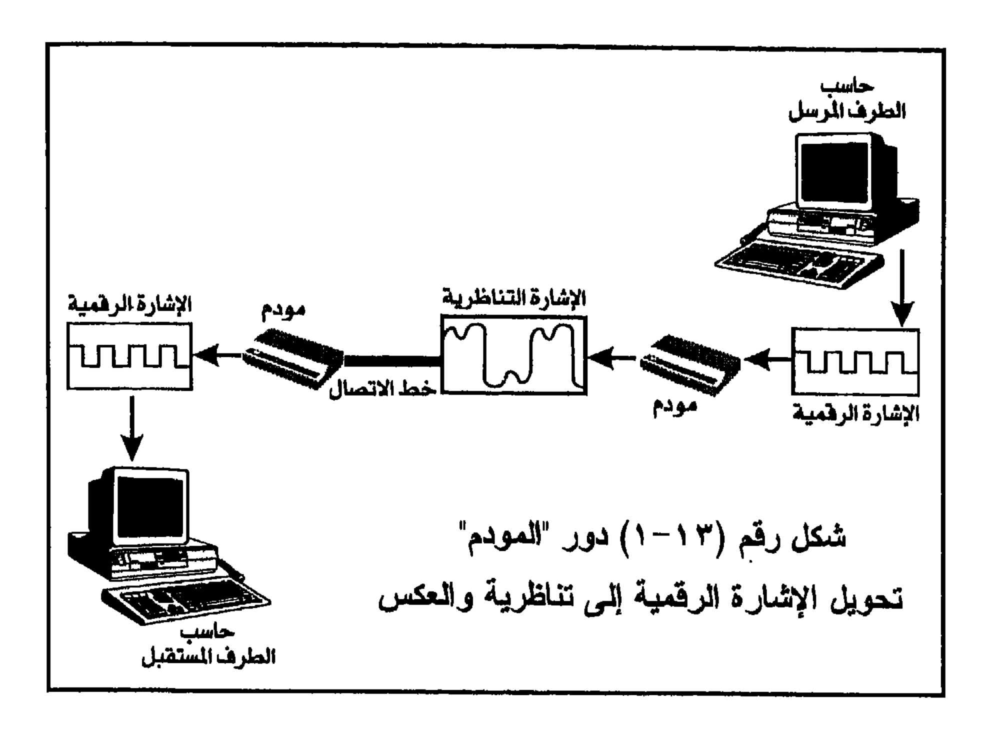
(٣) الأقمار الاصطناعية (Satellites).

٢-٥- الأجهزة المعاونة للاتصالات (Communication Interface Devices):

(١) "المودم" (Modem):

وهو الجهاز الذي يتولى تحويل البيانات الرقمية (Digital) التي يفهمها الحاسب إلي الصورة التناظرية (Analog) التي يمكن نقلها عبر

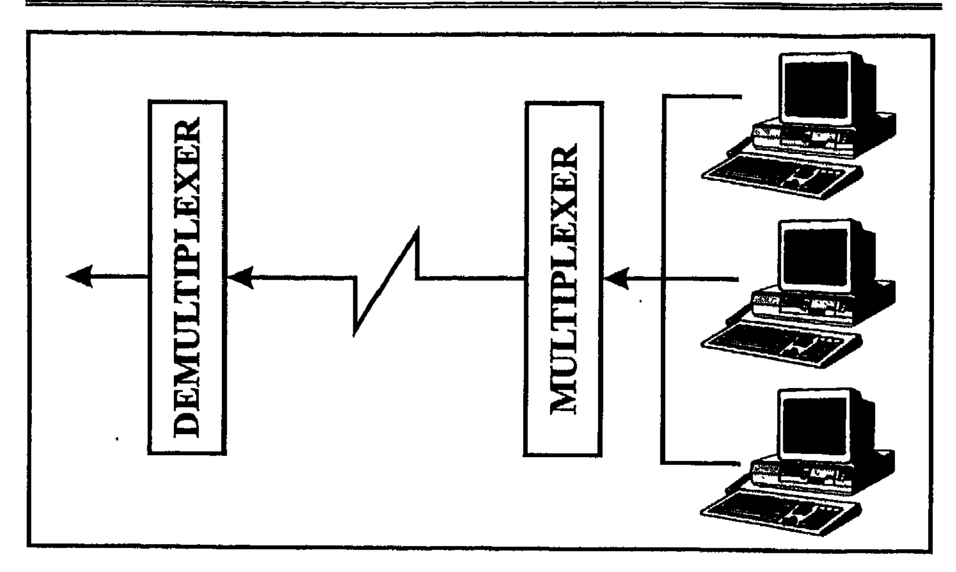
أسلاك الهاتف، وتسمى هذه العملية **التضمين (Modulation)** ثم يتولى إعادتها إلى الصورة الرقمية مرة أخرى عند نقطة الاستقبال، وتسمى هذه العملية **الكشف (Demodulation)**.



شكل رقم (١٣-١) دور "المودم"
تحويل الإشارة الرقمية إلى تناظرية والعكس

(٢) جهاز الاتصال المتعدد (Multiplexor):

وهو الجهاز الذي يمكن من استخدام خط اتصال واحد لنقل الرسائل المرسلة من عدة أجهزة، أو لاستقبال الرسائل الموجهة إلى أكثر من جهاز، إذ إنه ذو مداخل متعددة ومخرج واحد لتجميع الرسائل الواردة من عدة أجهزة (ذات سرعة بطيئة) وتوحيدها للمرور في خطٍ واحدٍ أكثر سرعة.



شكل (١٣-٢) استخدام جهاز الاتصال المتعدد (Multiplexor)

(٣) وحدة تحقيق التوازن (Equalizer).

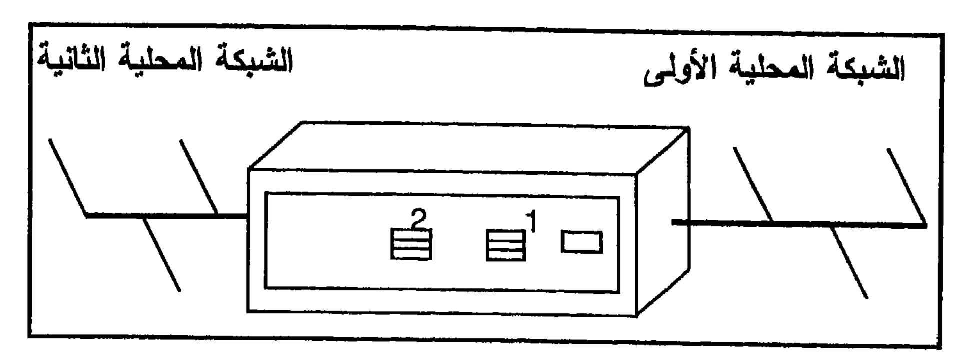
(٤) أجهزة التشفير وفك الشفرة (Encrypt / Decrypt).

(٥) المكررات (Repeaters):

وهي أجهزة تتيح مد الشبكة إلى عدة كيلومترات عن طريق إعادة توقيت وتوليد حزم البيانات (packets) لتتابع سيرها عبر المسافات الطويلة. وهذه الأجهزة رخيصة وسهلة التركيب ويمكنها الربط بين الأنواع المتباينة من الكوابل.

(٦) القناطر (Bridges):

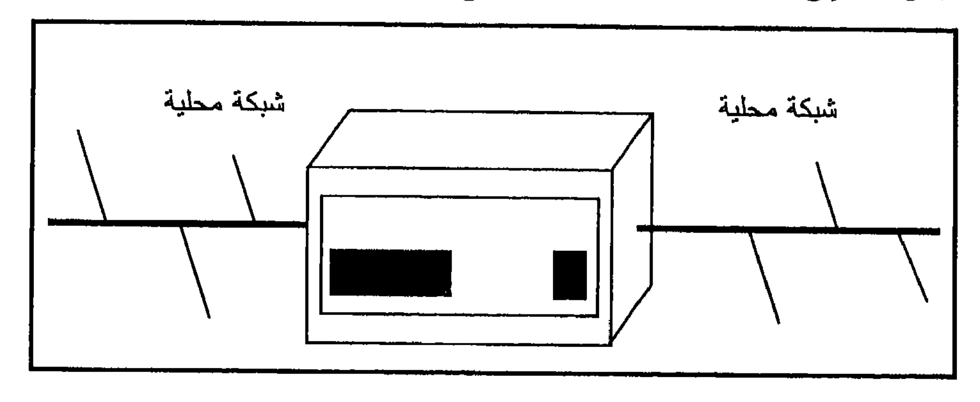
وتستخدم هذه الأجهزة لدمج شبكتين محليتين معًا بحيث تتمكن الحاسبات الموجودة في كلٍ منهما من استخدام مرافق (Resources) الشبكة الأخرى.



شكل رقم (١٣-٣) القناطر (Bridges)

(٧) الموجهات (Routers):

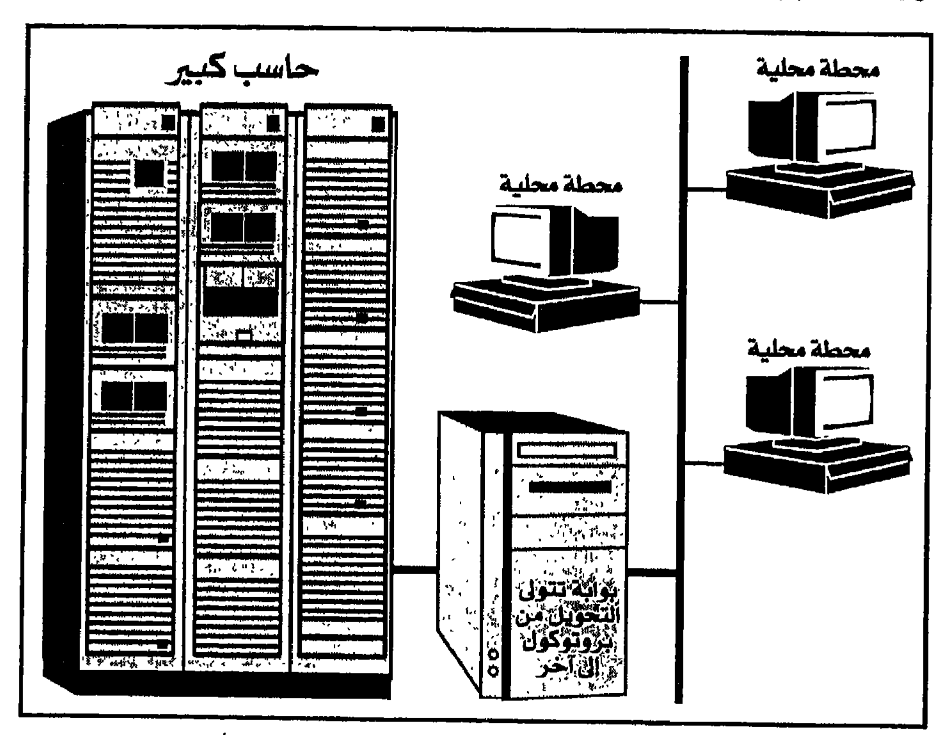
تتولى هذه الأجهزة الربط بين الشبكات التي تستخدم نفس البروتوكول، حيث تتولى الموجهات فحص عنوان كل رسالة فإذا كانت هذه الرسالة موجهة إلى محطة داخل نفس الشبكة فتقوم بتوجيهها إلى هذه المحطة، أمّا إذا كانت الرسالة موجهة إلى محطة خارج الشبكة فإنها تبعث بالرسالة إلى القنطرة المناسبة لنقلها خارج الشبكة.



شكل رقم (١٣-٤) الموجهات (Routers)

(٨) البوابات (Gateways):

وتستخدم لربط الشبكات المحلية بالحاسبات الكبيرة أو بالشبكات الأخرى، وهي تتيح الربط بين شبكات تستخدم بروتوكولات غير متوافقة، فعملها لا يقتصر على ربط الشبكات ولكنها تقوم كذلك بالتحويل من بروتوكول إلى آخر.



شكل رقم (١٣-٥) البوابات (Gateways)

٣- برامج تشغيل الشبكات ومراقبتها

يتم تشغيل الشبكات الكبيرة (WANs) والتحكم فيها ومتابعة أدائها من

خلال برامج تشغيل خاصة مثل: برنامج (Network Control Program) أو (NCP) من شركة "آي.بي.إم". وهذا البرنامج يتولى تنظيم تبادل المعلومات داخل شبكة يكون مركزها، أو أحد أطرافها، حاسبًا كبيرًا (Mainframe). وتتولى أنظمة التحكم في الشبكات بصفة عامة تنظيم تدفق البيانات من نقطة (node) إلى أخرى داخل الشبكة بمعدلات تتناسب وقدرات كل حاسب عضو في الشبكة، كما تنتج تقارير عن حالة الشبكة وكفاءة أدائها والمشكلات التي تتعرض لها، كما أن بها بعض البرامج التي تستخدم في حالة فقد البيانات ليمكن استعادتها وإرسالها مرة أخرى.

ومن برامج مراقبة أداء الشبكات برنامج "**أوميجامون**" **(OMEGAMON)** الخاص بمراقبة أداء الشبكات والذي يعطي مختص الاتصالات بمركز الحاسب الآلي صورة واضحة عن أداء الشبكة أولاً بأول (online)، ويمكن لمختص الاتصالات من خلال البرنامج معالجة المشكلات التي قد تحدث، كما يمكنه تشغيل أو تعطيل بعض الخطوط، أو تعديل سرعات البث، وهكذا ...

هناك كذلك برنامج **(NetView)** من شركة "آي.بي.إم" الذي يمكن من خلاله إدارة ومراقبة أداء الشبكات الكبيرة، ولدى شركة (AT&T) برنامج **(Accumaster Integrator)**، وهو جزء من نظامها المتكامل **(UNMA)** أو **(Unified Network Management Architecture)**.

وتستخدم بعض هذه البرامج لتوزيع التكلفة على كل مركز عضو في الشبكة وفقًا لاستخدامه للشبكة ولحجم البيانات التي يرسلها أو ترد إليه، بل يمكن كذلك تحديد تكلفة كل قسم أو إدارة وكل موظف، ويتم إنتاج هذه التقارير بمعدلات مختلفة وفقًا لما يحدده مختص الاتصالات.

ويعتبر أشهر بروتوكولات الشبكات حاليًا هو بروتوكول **(SNMP)** أو **(Simple Network Management Protocol)** ، وهو البروتوكول المستخدم في معظم الشبكات الرئيسية في العالم ، والذي تم تطويره من قبل

الحكومة الأمريكية والجامعة نفسها التي طورت بروتوكول **(TCP/IP)**. ويعمل بروتوكول (SNMP) بشكل جيد في شبكات وزارة الدفاع الأمريكية وجميع الشبكات العالمية التي تستخدم بروتوكول (TCP/IP) . ولأن النظم التي تستخدم بروتوكول (SNMP) منخفضة التكلفة ولا تلتهم الكثير من وقت المعالج المركزي فإن المتوقع أن ينتشر استخدام هذا البروتوكول في المستقبل.

٤- الأساليب الحديثة لنقل البيانات

٤-١- "بروتوكولات" الشبكات

إذا أردنا أن نرسل رسالة من مستخدم إلى آخر على الشبكة، وبرغم أن الحاسب الخاص بالمستخدم (ا) والحاسب الخاص بالمستخدم (ب) متصلان على نفس الشبكة فإن هناك أمورًا كثيرة يجب معالجتها مثل: **كيف يتصل كلٌ من الحاسبين بالخط المشترك؟ وكيف يتعرف كلٌ من الحاسبين على الآخر؟ وكيف ينبه أحدهما الآخر إلى أن هناك رسالة له؟ وماذا يحدث لو أن الحاسب (ب) كان مشغولاً جدًا ولا يمكنه استقبال الرسالة في الوقت الحالي؟** أمّا إذا كان الحاسبان في دولتين متباعدتين فهناك مشاكل أخرى مثل: **ما هو المسار الذي سوف تتخذه الرسالة بين الدولتين؟ وماذا يحدث في حالة تغير أساليب النقل المتعارف عليها دوليًا؟** وبفرض أن البيانات يتم نقلها بواسطة القمر الاصطناعي، **فكيف يتم تنفيذ ذلك؟ وماذا يتعين أن يتم في حالة فقد البيانات؟ وكيف يمكن حماية الرسائل وتأمينها والتأكد من عدم استقبالها بواسطة شخص غير مختص؟**

كل هذه الأمور التي أثرناها في صورة أسئلة تحتاج إلى اتفاقات (بروتوكولات) تتم لتوحيد أسلوب التعامل مع كل هذه المسائل. ومن أشهر أمثلة البروتوكولات بروتوكول (SNA) من "آي.بي.إم" وبروتوكول (DNA)

من "ديجيتال" ، وكلٌ منهما عبارة عن مجموعة من السياسات والمفاهيم والقواعد التي تتبع لتصميم وإدارة شبكات الحاسب والأجهزة المتصلة بها. وقد طور الجيش الأمريكي كما سبق الذكر بروتوكولاً خاصًا به هو بروتوكول (TCP/IP) أو (Terminal Control Program / Internet Protocol) كبروتوكول مستقل يستخدم لتوصيل الطرفيات (أو الحاسبات الشخصية) بالحاسبات الكبيرة.

وبعد انتشار الحاسب الشخصي ظهرت بروتوكولات من مثل: "إيثرنت" (Ethernet) و (PCLAN)، ثم استخدمت شركة (نوفيل) بروتوكول (SPX/IPS) في تطوير نظام التشغيل "نتوير" (Netware). ثم ظهر نموذج (OSI) وهو لا يعتبر في حد ذاته بروتوكولاً بالمعنى المفهوم ولكنه يحدد المسائل التي يتعين على أي بروتوكول معالجتها، وهو مرن بصورة تكفي لاستيعاب التقنيات الحديثة في المستقبل فمن الممكن تطبيقه على الشبكات الكبيرة (WANs)، أو شبكات المناطق (MANs)، أو الشبكات المحلية (LANs). وأصبح هذا النموذج وسيلةً معترفًا بها لتحديد وظائف جميع مكونات الشبكة والعلاقات بينها.

ومن أكثر نظم الشبكات انتشاراً في الوقت الحالي نظام (SNA) أو (System Network Architecture) ، وهو عبارة عن أسلوب بناء نظم نقل البيانات وهو بذلك يتضمن عدة بروتوكولات، ويشبه نموذج (OSI).

٤-٢- إرسال حزم البيانات (Packet switching)

تقوم (شبكات نقل حزم الرسائل Packet switching networks) بنقل الرسائل بعد تقسيمها إلى عدة (**حزم packets**) ذات حجم ثابت. وتتكون هذه الشبكات من مجموعة من القنوات التي تصل بين (**نقاط الشبكة Nodes**) أو من مقاسم تدار بواسطة الحاسب الآلي.

يتم أولاً تقسيم الرسالة المنقولة (سواء كانت بيانات رقمية أو صوت أو صور) إلى حزم بحيث يتصدر كل حزمة مقدمة (Header) تحتوي على معلومات عن الجهة المرسلة والجهة المستقبلة وعن ترتيب الحزمة ضمن الرسالة وغير ذلك من المعلومات ، ثم ترسل كل حزمة إلى الوجهة المطلوبة خلال أسرع الطرق المتاحة في تلك اللحظة (ولا يهم أن تصل الحزم إلى وجهتها بالترتيب الصحيح) ويعني ذلك أن حزم الرسالة الواحدة قد تمر عبر مسارات مختلفة إلى الوجهة المطلوبة حيث يتم هناك تجميعها بالترتيب الصحيح، وفقًا للمعلومات المبينة في مقدمة الرسالة، ومن ثم إيصالها إلى المستفيد. وتكون الشبكة في هذا الأسلوب مفتوحة لجميع المستفيدين طوال الوقت، فتجد حزم الرسائل القادمة من مختلف الجهات تتداخل داخل الشبكة ولكن كل منها تعرف طريقها إلى الجهة المستفيدة.

ويتيح هذا الأسلوب استخدامًا أفضل للشبكة، فباستخدام أحجام صغيرة للحزم واستخدام عدة بدائل للمسارات يمكن أن تتحقق موازنة الحمل في الشبكة بإعادة توجيه الحزم عبر الشبكة. كما يمكن من خلال هذا الأسلوب الوصول إلى الطاقة القصوى لوسائل الإرسال الرقمية عن طريق إرسال البيانات الرقمية من عدة جهات في الوقت نفسه على قناة اتصال واحدة.

في عام ١٩٨٠م أعلنت المواصفة القياسية (CCITT) الخاصة بشبكات نقل حزم البيانات والمعروفة باسم X.25 ولذلك كثيرًا ما يطلق على هذا النوع من الشبكات اسم شبكات (X.25) ، وقد طور هذا النوع من الشبكات إلى نظام **نقل الأطر** (**Frame relay**) ثم بعد ذلك إلى نظام (**ATM**) أو (**Asynchronous Transfer Mode**).

٤-٣- نظام نقل الأطر (Frame relay)

هو الأسلوب المنبثق عن نظام (ISDN) والذي صمم ليوفر نقل الأطر بسرعات عالية بأقل قدر من التأخير وبأفضل استخدام لمجال التردد

(Bandwidth) ، والإطار هو مجموعة من بيانات الرسالة حيث يتم تقسيم الرسالة إلى عدة أطر ، ويمكن استخدام هذا الأسلوب في الشبكات المحلية وفي النقل بأسلوب تقسيم الوقت (TDM) أو (Time Division Multiplexing) وكذلك في شبكات نقل حزم البيانات. وفي هذا الأسلوب يتم إرسال الإطار إلى الجهة المحددة في حقل العنوان الموجود ضمن الإطار نفسه، وفي هذا الأسلوب لا توجد ضرورة للتعرف على تمام وصول الرسالة أو إعادة الإرسال.

وهذا الأسلوب آخذ في الانتشار على حساب شبكات نقل حزم البيانات وإن كان المستقبل لنظام (ATM) أو (Asynchronous Transfer Mode).

٤-٤- نظام ATM (Asynchronous Transfer Mode)

فرض انتشار تطبيقات الوسائط المتعددة (Multimedia) الحاجة إلى نقل كميات هائلة من البيانات بسرعات عظيمة مما نقل التحدي إلى مجال الاتصالات، ومن هنا ظهر نظام (ATM) في معامل (AT&T) في بداية الثمانينيات من القرن العشرين ليمكن نقل الصوت والبيانات في الحزمة نفسها. وتم تعميم استخدامه في نهاية الثمانينيات من القرن الماضي ليستخدم في شبكات (ISDN) واسعة النطاق.

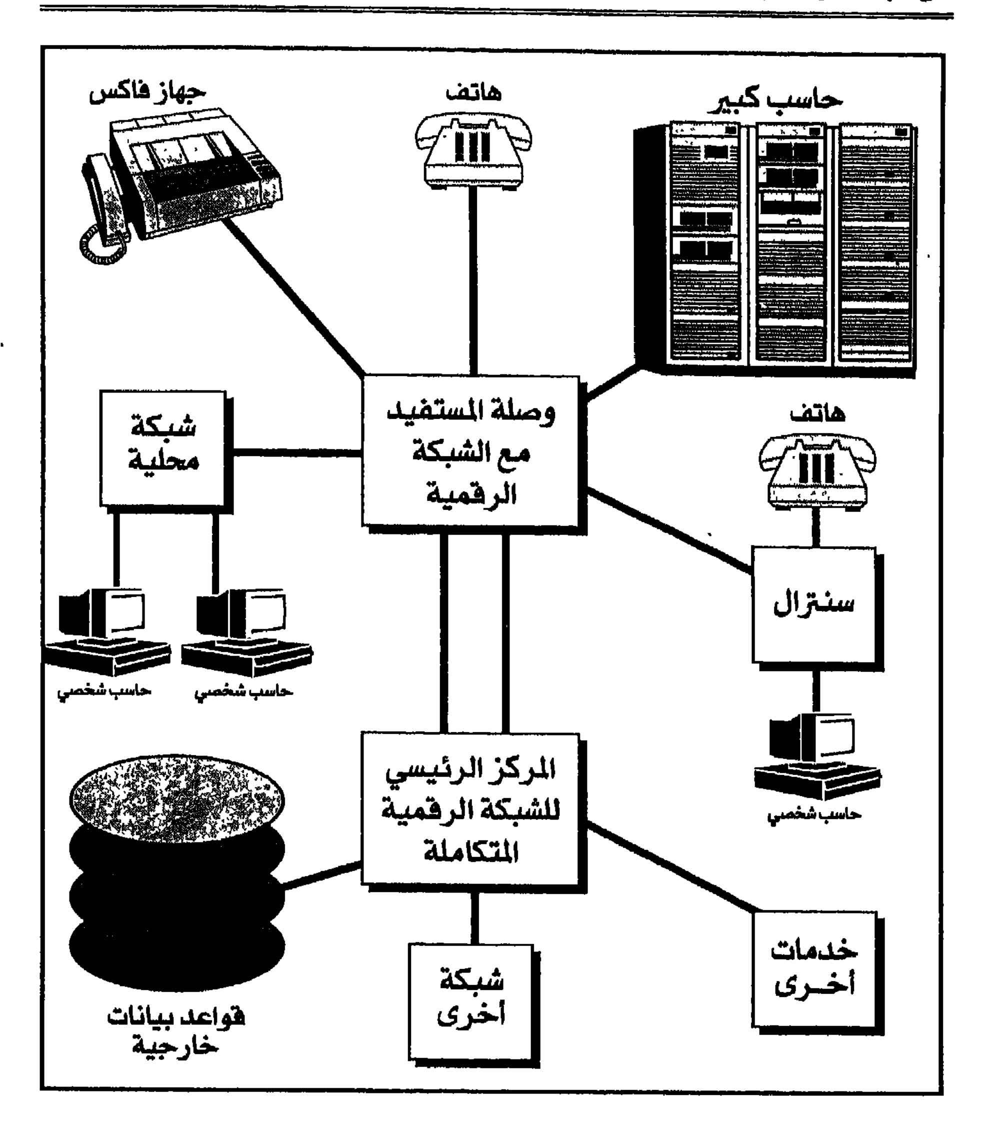
يستخدم هذا النظام حزمًا صغيرة ثابتة الحجم تسمى الخلايا (Cells) وقد أدى ثبات حجم الخلايا إلى سهولة تصميم النظام وإلى تقليل تأخير المعالجة (Processing delay) وكذلك تقليل اختلاف مدة التأخير (Variance of the delay) وهو الأمر الأساسي عند نقل خدمات حساسة للزمن مثل الفيديو والصوت. ويبلغ حجم الخلية (٥٣) بايت منها (٥) بايت كمقدمة (Header).

وسيتيح هذا النظام ــ بإذن الله ــ الدعامة التي تعتمد عليها الشبكات الرقمية واسعة النطاق للخدمات المتكاملة (BISDN) في المستقبل حيث تتراوح السرعات من (١٥٥) ميجا بت في الثانية إلى (٦٢٢) ميجا بت في الثانية وأكثر من ذلك بكثير.

٤-٥- الشبكة الرقمية للخدمات المتكاملة

Integrated Services Digital Network (ISDN)

بسبب اختلاف أسلوب النقل الرقمي عن أسلوب النقل التناظري، وبسبب اختلاف خصائص النقل بالنسبة لكل من الصوت والبيانات والصور والفيديو فقد أُنشئت لكلٍ من هذه الوسائل شبكاتٌ خاصة وأجهزةُ بثٍ خاصة، فأصبحت هناك شبكات تناظرية وأخرى رقمية، شبكات لنقل الصوت والبيانات وشبكات لنقل "الفاكسيميلي" وشبكات للتليفزيون و"الفيديوتكست" وشبكات مجال تخصصها هو (الائتمار عن بعد Teleconferencing) وغيرها. والسبب وراء هذا التعدد هو أن التقنيات اللازمة لنقل هذه الأشكال المتعددة للمعلومات لم تكن متاحةً، ولهذا ظهرت الحاجة إلى شبكة رقمية تقدم الخدمات المتكاملة لتحل محل هذا الخليط من الشبكات المتخصصة وليمكن نقل الصوت والبيانات والصور وأفلام الفيديو معًا بعد تحويلها إلى الحالة الرقمية. وهكذا ظهرت "الشبكة الرقمية للخدمات المتكاملة" (ISDN).



شكل رقم (١٣-٦) الشبكة الرقمية للخدمات المتكاملة (ISDN)

٥- مصادر تهديد البيانات خلال مرورها بالشبكات

٥-١- الأخطار التي تتعرض لها البيانات المنقولة

مهمة تأمين البيانات والحفاظ على سلامتها تكون سهلةً نسبيًا إذا كنا نتحدث عن حاسب واحد أو عن عدة حاسبات داخل غرفة أو مؤسسة واحدة، ولكن عندما تخرج البيانات لتنتقل عبر شبكة، سواء بمرورها في كوابل أو بانتشارها في الهواء، تزداد مشكلة تأمينها تعقيدًا، فالبيانات في هذه الحالة معرضة لبعض الأخطار، مثل:

١) فقد البيانات المرسلة.

٢) وصول البيانات إلى جهة أخرى.

٣) حدوث خطأ أو تحريف في البيانات خلال انتقالها.

٤) اختراق الشبكة (Hacking) إما للحصول على معلومات أو للتخريب المتعمد.

٥-٢- وسائل اختراق الشبكة

هناك وسائل عديدة تؤدي لاختراق الشبكة منها:

١) استخدام كلمات مرور بسيطة وسهلة الكسر.

٢) الاقتحام من خلال خطوط المراقمة (Dialup):

زاد تقدم التقنية مؤخرًا من تفاقم هذه المشكلة حيث يمكن الحصول على أجهزة مودم بسيطة وتركيبها في حاسب شخصي في المنزل مما يمكن من الدخول إلى الشبكات الكبيرة بسهولة. ولكن يوجد الآن أنواع من المودم التي تستخدم خاصة إعادة الاتصال (Dial back) لمعالجة هذه المشكلة حيث يقوم الحاسب الكبير بإعادة الاتصال بالمستفيد بعد اتصاله بالحاسب.

٣) اختراق خط الاتصال (Line tapping):

حيث يتم الدخول إلى الكابل الذي ينقل المعلومات بواسطة المقتحم للتنصت

على المعلومات المتبادلة أو لتغييرها سواء بعمل وصلة في الكابل أو بالحصول على الإشعاع غير المباشر الذي يبثه الكابل نفسه. ويتم التغلب على ذلك بتشفير البيانات المنقولة أو العزل الجيد للكابلات أو باستخدام كابلات الألياف الزجاجية التي تتميز بحصانتها العالية ضد الاختراق وضد تسرب الإشعاع.

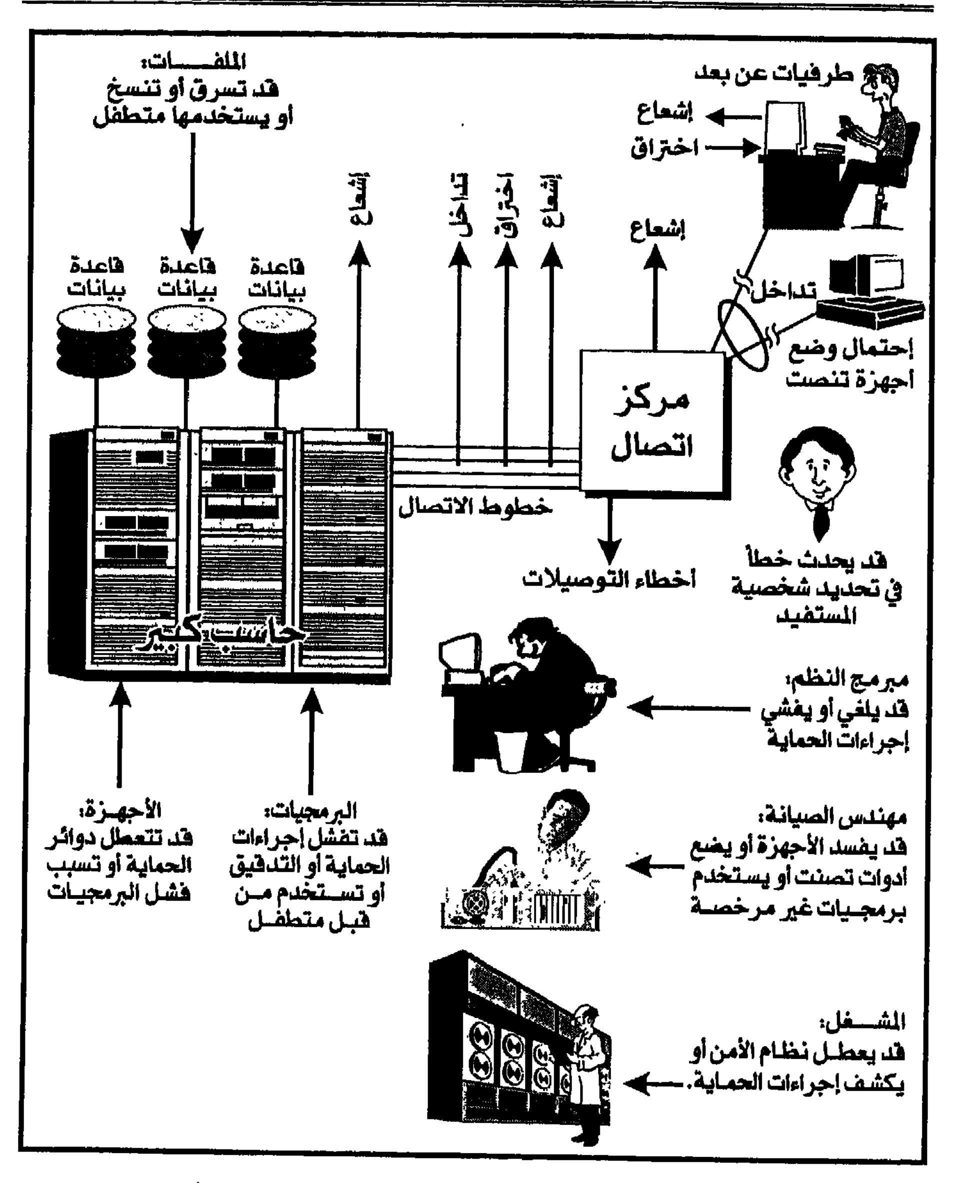
٤) إقحام الفيروسات في الشبكة:

ويتم هذه الجريمة إما عمدًا لإصابة الحاسبات المشتركة في الشبكة، أو بسبب إهمال القائمين على أمر الشبكة وعدم اتباعهم للإجراءات الضرورية لحماية الشبكة.

تتعرض الشبكة بالكامل لأخطار تهدد البيانات المارة بها في جميع المراحل بدءاً من نقطة إدخال البيانات وحتى وصول هذه البيانات للمستقبل. ويبين الشكل رقم (١٣-٧) النقاط المختلفة المعرضة لأخطار تهديد البيانات.

٥-٣- اختراق شبكة البنتاجون

ولا تنجو أكبر الشبكات في العالم من أخطار الاختراق فقد نشرت صحيفة نيويورك تايمز في عددها الصادر في ٥ مارس ١٩٩٩م أن المتحدث باسم البنتاجون الأمريكي (وزارة الدفاع) قد أعلن في اليوم السابق أن مختصي أمن المعلومات فيه قد نجحوا مؤخرًا في إفشال عدة محاولات لاقتحام شبكات البنتاجون المفتوحة والمرتبطة بشبكة إنترنت العالمية. كما أكد أن هناك المئات من المحاولات التي تتم أسبوعيًا لاقتحام شبكات البنتاجون وأجهزة الكمبيوتر فيه وأن معظم هذه المحاولات تتم فقط من أجل التفاخر بالقدرة على اقتحام شبكات البنتاجون. ولكنه أكد أن ٩٩,٩٥% من هذه المحاولات قد فشلت في الوصول إلى ما هو أبعد من الشبكة المفتوحة ومن ثم لم تشكل أي تهديد للأمن القومي الأمريكي.



شكل رقم (١٣-٧) النقاط التي يحتمل حدوث الخطأ فيها

٥-٤- الأخطار التي تهدد الشبكات والإجراءات المضادة

يبين الجدول (١٣-١) ملخصًا لأهم الأخطار التي تهدد الشبكات وآثار هذه الأخطار والإجراءات المضادة التي يتم اتخاذها لمواجهة هذه الأخطار:

الأخطار التي تهدد الشبكات وآثارها والإجراءات المضادة (٢/١)		
الخطر	الأثر	الإجراء المضاد
تعطل النهاية الطرفية	• انقطاع الخدمة. • تلف البيانات.	• الصيانة الوقائية. • طرفيات احتياطية.
السرقة أو التدمير	• انقطاع الخدمة.	• استخدام الأقفال. • التأمين على البيانات والمعدات. • إجراءات مادية لتنظيم الدخول. • مراقبة جيدة للمنطقة.
الاستخدام غير المصرح به للطرفيات	• تلف البيانات. • إفشاء بيانات سرية. • سرقة المعلومات.	• إجراءات مادية لتنظيم الدخول. • إجراءات (LOGON) حازمة. • صلاحيات محددة لكل مستخدم. • أساليب حديثة لتحديد الشخصية.
حصول غير المصرح لهم على المعلومات	• إفشاء بيانات عن أشخاص أو عن العمل.	• تحديد أماكن وجود الطرفيات. • استخدام قوائم التطبيقات (MENUS). • إجراءات مادية لتنظيم الدخول. • تمزيق المخرجات الورقية.
أعطال الخطوط أو أجهزة الموديم	• انقطاع الخدمة. • تلف البيانات.	• تشخيص الأعطال. • وجود بدائل للخطوط والمودم. • أساليب اكتشاف وتصحيح الأخطاء (Error Detection & Correction).
مهاجمة الخطوط أو مراكز الاتصال	• انقطاع الخدمة.	• إجراءات مادية لتنظيم الدخول. • خطوط بديلة. • دفن الخطوط في باطن الأرض وعزلها جيدًا.

الأخطار التي تهدد الشبكات وآثارها والإجراءات المضادة (٢/٢)		
الخطر	**الأثر**	**الإجراء المضاد**
التشويش على الإشارات المنقولة	• انقطاع الخدمة. • تشوه البيانات.	• العزل الجيد للكوابل. • استخدام مرشحات لتنقية الإشارات.
الاقتحام	• حصول غير المرخص لهم على بيانات سرية.	• تشفير البيانات. • تطبيق الإجراءات المادية لتأمين المنشأة. • مراقبة الخطوط.
تعطل وسيلة نقل البيانات	• انقطاع الخدمة.	• مسارات بديلة. • استخدام خاصة التحول الآلي للخط المراقم المؤقت (Auto Dialup) أو (Fallback).
تعطل بعض الأجهزة	• انقطاع الخدمة.	• أجهزة احتياطية. • استخدام القناطر في الشبكات.
أعطال البرمجيات	• انقطاع الخدمة. • عدم الثقة في سلامة البيانات.	• استخدام برمجيات معالجة الأعطال. • استخدام برمجيات استعادة النشاط.
أخطاء التشغيل	• عدم الثقة في سلامة النظام ككل.	• وجود نسخة أخرى من البيانات. • استخدام بدائل احتياطية.

جدول (١٣-١) ملخص الأخطار التي تهدد الشبكات وآثارها والإجراءات المضادة

٦- ضمان صحة البيانات المرسلة

لابد للبيانات المرسلة عبر الشبكة أن تصل إلـــى الجهـــة المســـتهدفة بالضبط، وأن تصل صحيحة ودقيقة وكاملة الأجزاء وفي الوقت المطلـــوب تمامًا، ولابد كذلك أن تصل مرةً واحدة بلا تكرار.

يتم التأكد من صحة البيانات المرسلة عبر الشبكة بالتأكد من شـــخصية المرسل وصلاحياته في الإرسال، والتأكد من محتوى الرسالة المرسلة وأنـــها لم تتعرض لأي خطأ متعمد أو عفوي.

٦-١- تحديد شخصية المستخدم (Personal identification)

يعتبر هذا هو خط الدفاع الأول للتأكد من صلاحية المستخدم في بـــث البيانات. ويتم ذلك بأحد أسلوبين نوردهما هنا كمجرد مثلين فقـــط لأســـاليب التأكد من شخصية المستخدم وهي كثيرة:

٦-١-١- استخدام كلمات المرور (Passwords)

وهذا هو أسهل أسلوب وأرخص أسلوب كذلك، ولكـــي يحقـــق هـــذا الأسلوب النجاح يجب توعية المستخدمين بعدم التخلي عن كلمة المرور لأي شخص، وأن يفرض عليهم تغييرها بصفة دورية. ويجب كذلك تشفير كلمات المرور في الملفات المستخدمة لحفظها في الحاسب، وعنـــد إدخـــال كلمـــة المرور لا يجب أن يعرض النظام حروفها حتى لا تنكشف أمام المتطفليـــن. كما تتبع بعض الجهات أسلوب تخصيص كلمات المرور بواســـطة مختـــص الشبكة أو مسئول أمن النظام ، وذلك لتلافي المحاولات البسيطة لتخمين كلمة المرور التي قد تكون اسم أحد أبناء المستخدم أو تاريخ ميلاده مثلاً.

ومن عيوب هذا الأسلوب أنه يمكن كسره بسهولة بواسطة برامج تقوم بعمل عدد لانهائي من المحاولات حتى تتوصل إلى الكلمة الصحيحة، ولذلك يجب تحديد عدد المحاولات الفاشلة التي يتم بعدها فصل الطرفية وإيقافها عن العمل تمامًا.

٦-١-٢- إعادة الاتصال (Call back security)

بعد أن أصبح الآن من الشائع اتصال المستخدمين عن بعد بالحاسب الرئيسي ومن ثم الدخول إلى الشبكة، ففي هذا الأسلوب يتصل المستخدم برقم هاتف آخر غير رقم هاتف الشبكة، وفي هذه الحالة يقوم النظام بإعادة الاتصال برقم هاتف المستخدم المسجل في ذاكرة خاصة ضمن قائمة هواتف المستخدمين المرخص لهم. ولكن يعيب هذا الأسلوب ضرورة اتصال المستخدم من هاتف محدد (أو عدة هواتف محددة مسبقًا)، وعند الازدحام يتم وضع المستخدم في قائمة الانتظار ويتم تحديد أولويته وفقًا لمعايير كثيرة، وعند وجود خطٍ خالٍ يتم الاتصال بالمستفيد.

٦-٢- تدقيق محتويات الرسالة (Message validation)

لكي يمكن تدقيق محتويات الرسالة بسهولة يفضل وضع معايير ثابتة للرسائل المتوقع تبادلها عبر الشبكة بين الأطراف، بحيث تكون لها صيغة معيارية يمكن اختبارها للتأكد من أن هذه الرسالة هي إحدى الرسائل المتوقع مرورها عبر الشبكة، ومن نقاط التحقق الشائعة:

١) وجود بيانات محددة كأن تبدأ الرسالة بتاريخ الإرسال وتحديد هوية المرسل.
٢) أن تحمل الرسالة إجمالي الحقول الرقمية في نهاية هذه الحقول للتأكد من صحة إرسال الأرقام.

٣) استخدام خانة التدقيق (Parity check) وبعض الأرقام الاختبارية أو الكلمات المتفق عليها، ويجب في هذه الحالة إخطار المرسل بنتيجة تدقيق رسالته.

٦-٣- توصيل الرسالة (Message delivery)

عند وصول الرسالة يتم التأكد في جهة الوصول مما يلي:

١) أن الرسالة وصلت من جهة صحيحة مرخص لها بالإرسال، وأنه قد تم حدوث اتصال بين نقطتي الاتصال قبل لحظة الإرسال.

٢) أنه لم يحدث تنصت على الخط وفي حالة حدوثه التأكد من أن البيانات مشفرة مما يمنع المتنصت من الاستفادة من محتويات الرسالة.

٣) أن كل أجزاء الرسالة قد وصلت.

٤) أنه لم يتم تزوير الرسالة أو تعديلها.

وتستخدم للتأكد من ذلك أرقام غير متكررة للرسائل، وهي ما نطلق عليها (USRN) أو (Unique System Reference Numbers).

٦-٤- حماية البيانات المرسلة

يجب توجيه مزيد من العناية للتدقيق على البيانات المهمة خلال إرسالها عبر الشبكة مثل: المبالغ المالية ورمز المرسل ورمز المستقبل وذلك لجميع الرسائل والتأكد من وصول كل أجزاء الرسالة وعدم وجود رسائل دخيلة أو أن جزءاً من الرسالة لم يصل بعد، أو أن الرسالة نفسها لم ترسل مرتين فهذا قد يسبب مشكلة كبيرة في حالة المعاملات البنكية مثلاً فقد ينتج عن ذلك إضافة المبلغ إلى الرصيد مرتين.

٦-٥- إعادة الإرسال في حالة فقد البيانات المرسلة

تتخذ في الشبكات الكبيرة بعض الاحتياطات لضمان وصول الرسائل إلى الجهة المستقبلة، وفي حالة تعثر وصول إحدى الرسائل يمكن تحاشي فقدها باستخدام الأنواع الحديثة من أجهزة المودم التي تنتظر تأكيدًا من الجهة المستلمة للرسالة بتمام وصول الرسالة، وفي حالة عدم تلقي هذه الإشارة يقوم جهاز المودم بإعادة إرسال الرسالة مرة أخرى، ويسجل النظام هذا الخطأ في سجل الأعطال (Log).

٦-٦- استخدامات الخطوط الخاصة (Leased lines)

الخطوط الخاصة (Leased lines) هي خطوط يتم تأجيرها من شركات الهاتف وهي تخصص بالكامل للاتصال بين نقطتين وتكون متاحة طوال الوقت لنقل البيانات بين هاتين النقطتين، فإذا لم يكن هناك اتصال تظل عاطلة عن العمل، وتضمن الجهة المستخدمة بذلك أقل قدر من التأخير في إرسال رسائلها مهما كان ازدحام خطوط الهاتف، ويعتبر استخدام الخطوط الخاصة إحدى الوسائل المستخدمة لتأمين البيانات ماديًا عن طريق تأمين مسار الخط الخاص.



الفصل الرابع عشر

أمن شبكات "إنترانت" المحلية

موضوعات الفصل:

(١) الشبكات المحلية وأنواعها.
(٢) مكونات الشبكات المحلية.
(٣) مفهوم "إنترانت".
(٤) وسائل تأمين المعلومات في الشبكات المحلية.
(٥) أمن البريد الإلكتروني في شبكات "إنترانت".



نتناول في هذا الفصل أمن شبكات "إنترانت" المحلية ، فنبدأ بمقدمة عن أنواع الشبكات المحلية، والأجهزة التي تتكون منها، ثم نعالج مفهوم "إنترانت".

نقدم بعد ذلك بعض وسائل تأمين المعلومات المتبادلة عبر هذا النوع من الشبكات، سواء باستخدام إمكانيات برامج تشغيل الشبكة أو باستخدام بعض البرامج المساندة ، أو باستخدام بعض الوسائل المادية في تحقيق الأمن والحماية للبيانات المتداولة عبر الشبكة.

نختتم الفصل بالحديث عن أمن البريد الإلكتروني الداخلي في شبكات "إنترانت"، وتعتبر هذه الخاتمة تمهيدًا مناسبًا للفصل التالي الذي خصصناه لمشاكل الأمن والحماية في الشبكة العالمية "إنترنت".

١- الشبكات المحلية وأنواعها

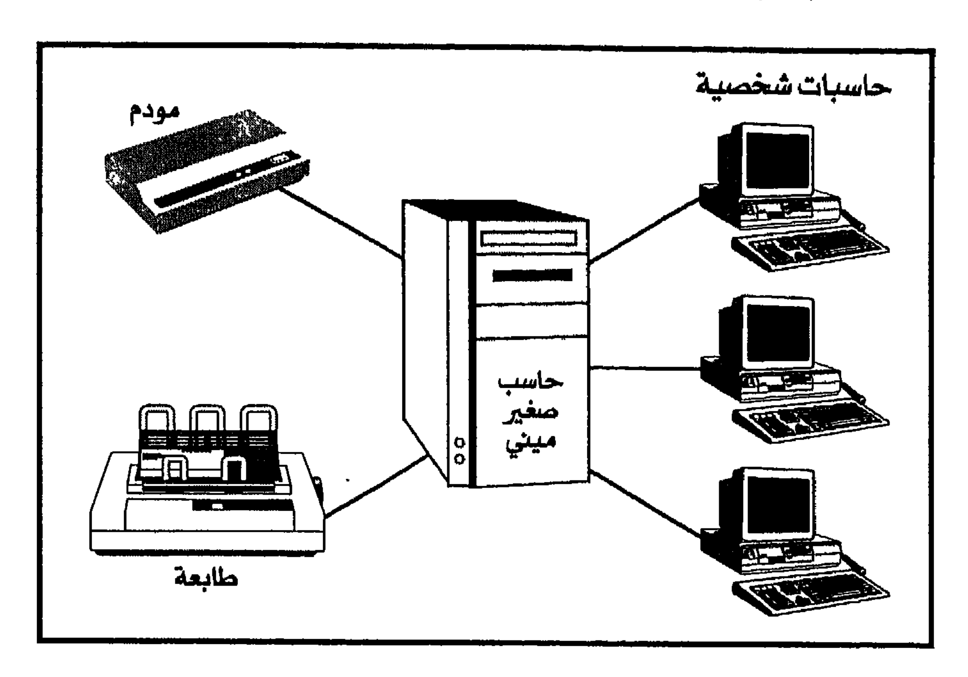
عندما نتحدث عن الشبكات المحلية فإننا نعني "**طبوغرافية" الشبكة** **(Network topology)**. وهذه "الطبوغرافية" هي إما أن تكون **مادية** **(Physical topology)** أي وصف المسار الذي تتبعه "كابلات" الشبكة للتوصيل بين نقاط الشبكة (nodes) وإما **منطقية** **(logical topology)** أي وصف طريقة سريان الرسائل بين هذه النقاط.

وأشهر أنواع الشبكات المحلية، مصنفة حسب "الطبوغرافية"، ثلاثة أنواع هي:

١-١ الشبكة النجمية (Star network)

في هذا النوع من الشبكات تتصل كل وحدة من وحدات الشبكة، عن طريق "كابل" منفصل، مباشرة بوحدة التحكم في الشبكة، أو "خادم الملفات" (File server) كما يبدو في شكل رقم (١٤-١).

وواضح أن هذا النوع يستلزم مد "كابل" من كل وحدة يصل إلى مركز الشبكة، فإذا كان من طبيعة الوحدات التي تضمها الشبكة كثرة الانتقال من مكان إلى آخر فهذا الأسلوب يكون مكلفاً، كما أنه إذا تعطل مركز الشبكة تعطلت الشبكة بالكامل.



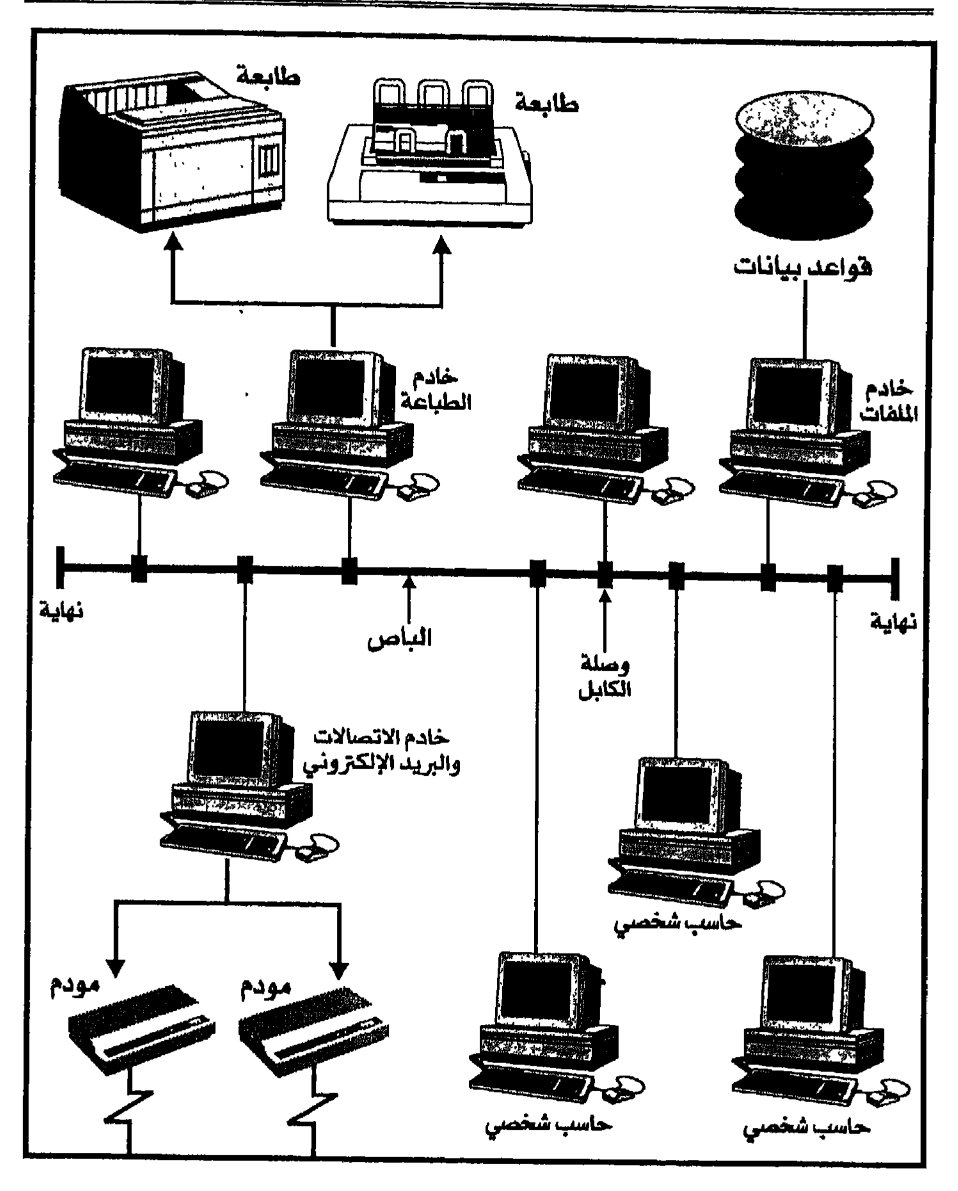
شكل رقم (١٤-١) الشبكة النجمية (Star network)

١-٢ الشبكة "الباص" (Bus network)

في هذا النوع من الشبكات تتصل جميع الوحدات بكابل واحد ويسمى "باص" (Bus) كما يبدو في الشكل رقم (١٤-٢). أي إن الوحدات المختلفة

بالشبكة يقوم على خدمتها "كابل" واحد، ولذلك يتعين أن تكون سرعة النقـــل لهذا "الكابل" كافية لاستيعاب حركة النقل بالشبكة.

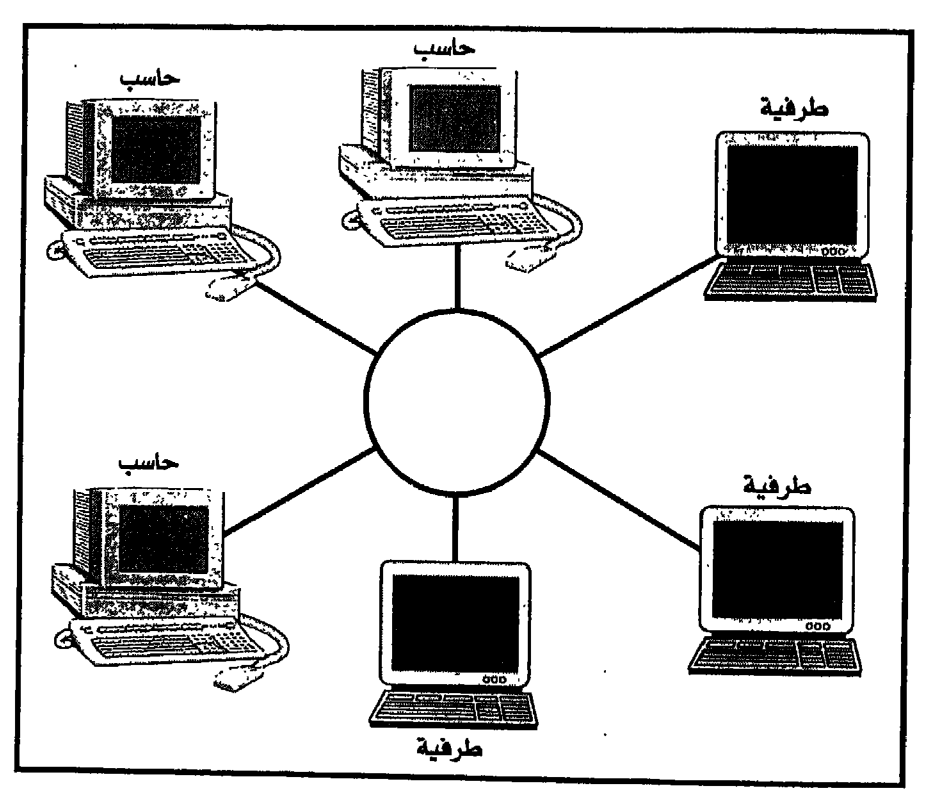
ومن مزايا هذا النوع من الشبكات سهولة إضافة وحـــدات جديـــدة أو نقلها من مكانها بمجرد مد "كابل" واحد قصير ووصله بالكابل الرئيسي عـــن طريق وصلات (Taps)، والوصلة هي جهاز صغير يتم تركيبه على "الكابل" بسهولة. وفي هذا النوع لا يتسبب تعطل الوحدة الرئيسية في تعطل الوحـدات المتصلة بالشبكة، ولكنها ستحرم من خدمات الشبكة.



شكل رقم (١٤-٢) الشبكة "الباص" (Bus network)

١-٣ الشبكة الحلقية (Ring network)

في هذا النوع من الشبكات يمر "كابل" يربط بين كل الوحدات المتصلة بالشبكة في حلقة واحدة كما يبدو في الشكل رقم (١٤-٣). فتقوم كل وحدة بالشبكة بتمرير أية رسالة إلى الوحدة المجاورة إذا لم تكن تخصها، وإذا تعطلت إحدى الوحدات استمرت الوحدات الأخرى في العمل وتمر الرسائل من خلال الوحدة المعطلة دون عرقلة.



شكل رقم (١٤-٣) الشبكة الحلقية (Ring network)

٢- مكونات الشبكة المحلية

إن العتاد الأساسي (Hardware) المطلوب لإنشاء الشبكة المحلية يتكون من خادم الملفات (File server) والحاسبات الشخصية المستضافة (Client stations) وبطاقات التوفيق (Network interface adapters) التي تركب في هذه الحاسبات بالإضافة إلى "الكابلات".

٢-١ خادم الملفات (File server)

يعتبر مركز الشبكة وهو قد يكون حاسبًا صغيرًا (Mini) أو حاسبًا شخصيًا ذا إمكانيات كبيرة من حيث السرعة وسعة القرص الصلب. ويقوم هذا المركز بإتاحة مرافقه من قرص صلب وطابعات وغيرها للحاسبات المستضافة (Clients). وأهم خصائص هذا الجهاز (Server) التي ينبغي الاهتمام بها هي سرعة القرص الصلب ففي الشبكات المزدحمة تكون هذه هي نقطة الاختناق الرئيسية.

٢-٢ الحاسبات الشخصية المستضافة (Client stations)

هي الحاسبات التي تشكل نقاط الشبكة (Nodes) والتي يستخدمها المستفيدون مباشرة.

٢-٣ بطاقات الربط بالشبكة (Network interface adapters)

يحتاج كل حاسب شخصي في الشبكة إلى بطاقة ربط بالشبكة وهي عبارة عن لوحة دوائر مطبوعة (printed circuit) فائدتها استقبال الإشارات

المتسلسلة القادمة عبر "كابلات" الشبكة وإيصالها إلى مدخل البيانات المتوازي داخل الحاسب الشخصي. كما تستطيع هذه البطاقة كذلك تغيير نسق البيانات من متوازٍ إلى متسلسل، وتضخيم الإشارات لتتمكن من تجاوز المسافة الضرورية.

٢-٤ (الكابلات Cables)

١) الزوج المجدول غير المعزول (Unshielded Twisted Pair).

٢) الزوج المجدول المعزول (Shielded Twisted Pair).

٣) "الكابل" المحوري (Coaxial cable).

٤) "كابل" الألياف البصرية (Fiber Optic Cable).

كما شاع في الآونة الأخيرة استخدام **الأشعة تحت الحمراء (Infrared rays)** في توصيل الشبكات المحلية لتلافي استخدام "الكابلات".

٣- مفهوم "إنترانت"

مع انتشار استخدام شبكة "إنترنت" العالمية ظهرت تقنيات كثيرة تستخدمها الشبكة، سواء في تقنيات التراسل عبر الشبكة أو تقنيات تأمين البيانات المنقولة عبرها أو تقنيات التشفير أو تقنيات "عرض البيانات" (Browsers) أو تقنيات "تصميم الصفحات الخاصة" (Home Pages) أو أساليب إنشاء "المواقع" (Sites) على الشبكة. وصاحب ذلك ظهور لغات خاصة لتداول المعلومات وعرضها على الشبكة العالمية مثل: "لغة معالجة النص الفائق" (HTML) أو (Hyper Text Manipulation Language) وكذلك مؤخرًا لغة (XML) ولغة (DHTML) التي تستخدم الرسوم المتحركة (Animation)، وتقنيات تصميم الصفحات مثل: برنامج "صفحة

الغلاف" (Front Page) من شركة مايكروسوفت ومبادرة شركة "صن" (Sun) ببرنامج (نت سكيب NetScape) لعرض البيانات الذي لم تتوانى شركة "مايكروسوفت" بعده عن إصدار برنامجها "مستكشف إنترنت" (Internet Explorer) الذي يؤدي الغرض نفسه.

بالإضافة إلى تقنيات أمنية أخرى مثل: (جدر الحماية Firewalls) و (الوسيط Proxy) وغيرها من تقنيات حماية البيانات داخل الشبكات أو التقنيات التي تستخدم لحظر الدخول إلى مواقع معينة على الشبكة.

جميع هذه التقنيات التي سبق ذكرها استفاد منها مصممو الشبكات المحلية فأصبحت الشبكات المحلية تستخدم جدر الحماية وتستخدم أساليب العرض (Browsers) وتصميم الصفحات وإعداد المواقع وغيرها. باستخدام هذه التقنيات المستعارة من شبكة "إنترنت" العالمية في الشبكات المحلية أطلق على هذه الأخيرة اسم (إنترانت Intranet) لتحمل مفهوم الشبكة المحلية ومفهوم استخدامها لتقنيات "إنترنت".

وما دمنا أطلقنا اسم "إنترانت" على الشبكات الداخلية فقد ظهر أيضًا مصطلح آخر وهو (إكسترانت Extranet) حيث يطلق على الشبكة الخارجية إذا كنا ننظر إليها من داخل شبكة "إنترانت"، أو ما يسمى (الشبكة الخاصة الافتراضية Virtual Private Network) أو باختصار (VPN).

وهكذا لم تمنحنا شبكة إنترنت العالمية فقط تقنياتها لنستخدمها في شبكاتنا المحلية ولكنها منحتنا أيضًا مجموعة من المصطلحات والمفاهيم الجديدة!

٤- وسائل تأمين المعلومات في الشبكات المحلية

٤-١ دور برامج تشغيل الشبكات المحلية

مهمة برامج التشغيل (أو أنظمة التشغيل) الرئيسية في الشبكة هي أن تجعل المرافق البعيدة عن الحاسب تبدو كمرافق محلية، فإذا كان المطلوب الوصول إلى الملفات المخزنة على القرص الصلب لحاسب بعيد فالنظام يسهل الوصول إليها، وكذلك الحال في الطابعات البعيدة فيمكن استخدامها وكأنها مركبة على منفذ التوازي الخاص بالحاسب الشخصي.

ولذلك تلعب نظم التشغيل دوراً مهمًا في تحقيق سلامة البيانات في الشبكات ويمكن تحديد هذا الدور في مجموعة من الإمكانيات نوضحها فيما يلي:

١) إعداد النسخ الاحتياطية للبيانات (Backup copies):

وقد سبق الحديث عن هذا الموضوع باستفاضة في الفصل العاشر (نظم أمن البيانات).

٢) تمييز المستخدم وتحديد صلاحياته

(User identification & authorization) :

ويتم ذلك من خلال (كلمات المرور Passwords) حيث يمكن تحديد المستخدمين وصلاحياتهم ، كما يمكن من خلال كلمات المرور توفير الحماية لعدد من المرافق مثل: القرص الصلب والأدلة الفرعية وحتى على مستوى الملف. كما يمكن استخدام عدة مستويات من الصلاحيات: (القراءة والكتابة والتعديل والإنشاء والحذف).

٣) تحديد صلاحيات استخدام الملفات :

حيث يمكن من خلال خصائص نظام التشغيل تحديد صلاحيات استخدام الملفات وتوزيع هذه الصلاحيات على فئات المستخدمين:

- القراءة فقط.
- القراءة والتعديل.
- الإنشاء.
- الحذف.

٤) تحديد صلاحيات استخدام المرافق:

يُعطى كل مرفق بالشبكة "اسم شبكة" وهذا الاسم قد يعطى لوحدة إدارة أقراص أو لفهرسٍ فرعي أو حتى لملفٍ واحد، ويمكن ربط كلمة مرور مع هذا الاسم لتحديد صلاحيات الاستخدام. ولكن يعيب هذا الأسلوب اضطرار المستخدم لتذكر العديد من كلمات المرور.

٥) تحديد صلاحيات مجموعات المستخدمين:

للتغلب على مشكلة تعدد كلمات المرور يتم تقسيم المستخدمين إلى فئات (أو مجموعات) بحيث ينتمي كل مستخدم لمجموعة معينة أو أكثر ويحدد لكل مجموعة صلاحيات استخدام معينة، وبالتالي يكون كل شخص مسئولاً عن كلمة مرور واحدة، وفي هذا الأسلوب يمكن نقل المستخدم من مجموعةٍ إلى أخرى بسهولة.

٦) إجازة الأعطال (Fault tolerant):

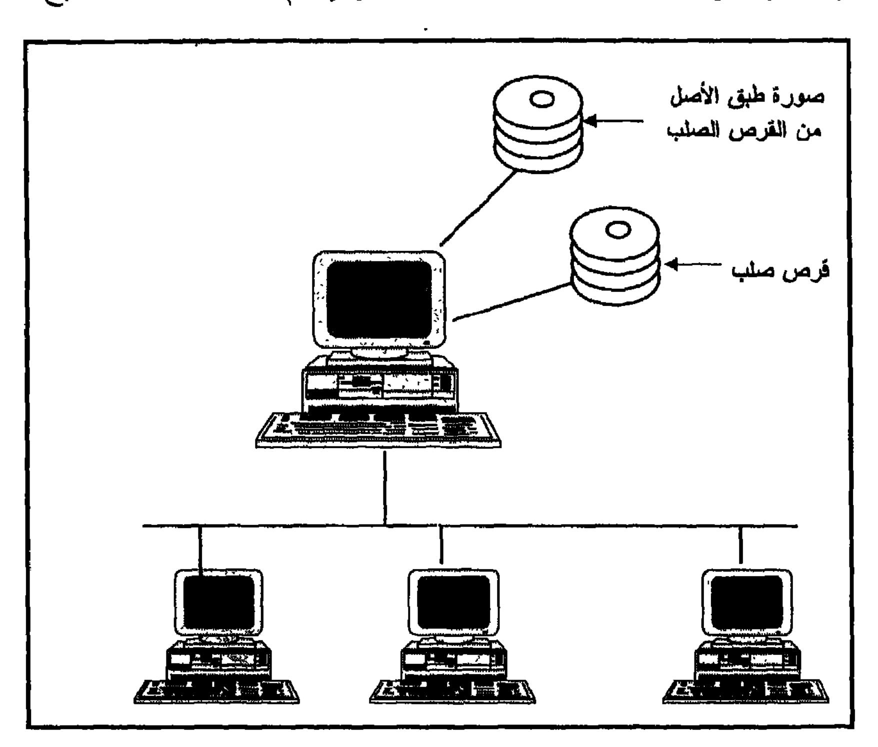
ويتم ذلك بإنشاء صورة طبق الأصل من الملفات (Mirror) أو من القرص الصلب في خادم الملفات بإضافة قرص احتياطي.

٧) **تشخيص الأخطاء (Diagnosis programs):**

يقوم هذا النوع من البرامج بتحديد وتشخيص الأخطاء التي تقع.

٨) **تدقيق القراءة بعد الكتابة (Read-after-write verification):**

يقوم هذا النوع من البرمجيات بإعادة قراءة البيانات بعد كتابتها على القرص ومقارنتها بالبيانات الأصلية للتأكد من إتمام الكتابة بشكل صحيح.



شكل رقم (١٤-٤) استخدام صورة مطابقة من الملفات أو القرص الصلب

٤-٢ اختيار أنظمة التشغيل

عند اختيار نظام التشغيل المناسب للشبكة يجب الالتفات إلى العوامل الفنية التالية إلى جانب العوامل الأخرى مثل: السعر ودعم الشركة المورردة وغير ذلك:

١) العدد الأقصى المتوقع من الحاسبات الشخصية المستضافة.

٢) هل هناك حاجة لخلط حاسبات ذات طرز مختلفة ضمن الشبكة (مثل خلط حاسبات "ماكنتوش" مع حاسبات "آي.بي.إم")؟

٣) هل هناك حاجة لخلط حاسبات تستخدم نظم تشغيل مختلفة ضمن الشبكة، مثل: (UNIX) أو (VMS) مع (DOS) مثلاً؟

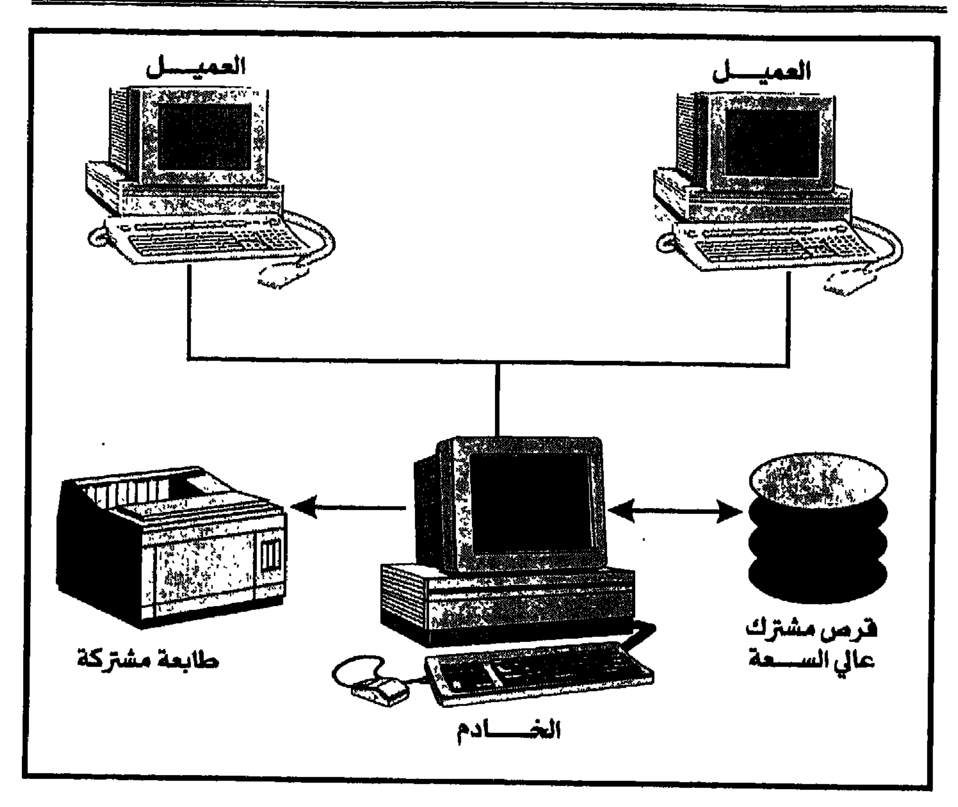
٤) هل هناك حاجة لربط الشبكة المحلية عبر خطوط الهاتف مع شبكات أخرى أو حاسبات بعيدة؟

٤-٣ دور البرامج المساندة في تأمين الشبكات المحلية

البرامج المساندة لنظم تشغيل الشبكات (Network utilities) هي برامج خاصة مضمنة في نظام التشغيل وهي تقوم بإنجاز مهام معينة للمستخدم ومن هذه البرامج المساندة :

١) البرامج المساندة لإدارة خادم الملفات:

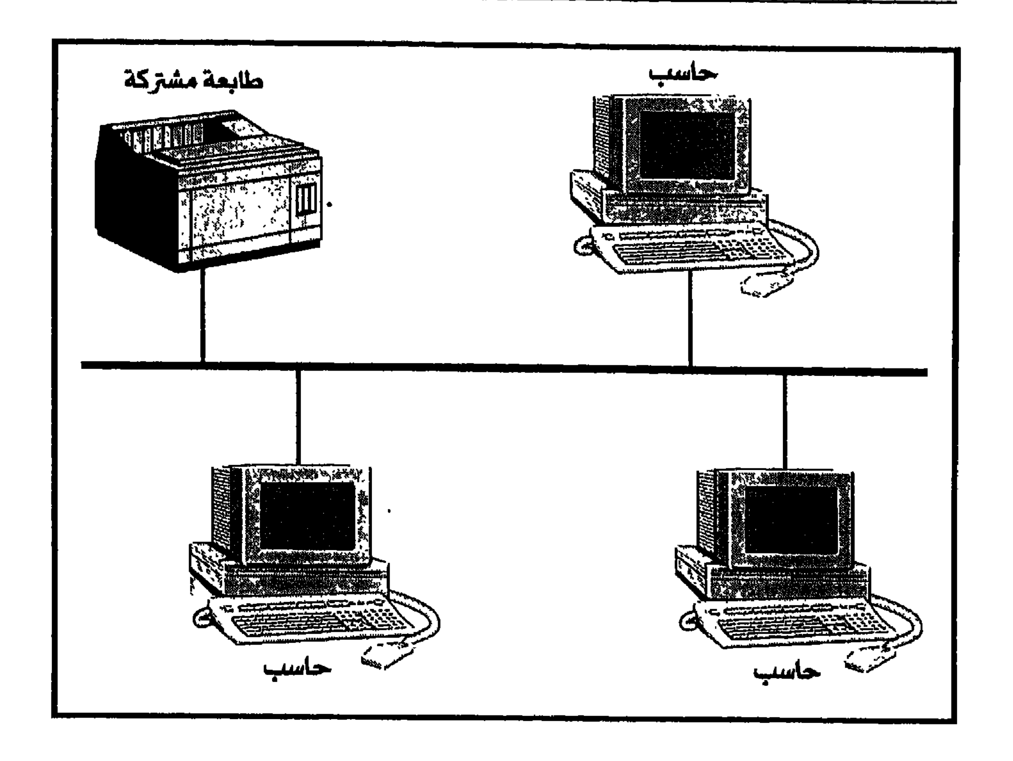
وهذه البرامج تمكن المستخدم من استخدام القرص الصلب في خادم الملفات وتتيح له بناء **الفهارس المنطقية** **(Logical Directories)** على هذا القرص.



شكل رقم (١٤-٥) استخدام القرص الصلب المشترك

٢) البرامج المساندة لإدارة الطباعة:

وهي تمكن المستخدمين من الطباعة على طابعة مشتركة، فالبرنـــامج المساند (Spool) يسمح للحاسب الشخصي بإرسال بيانات إلى ذاكرة وسـيطة للطابعة (Printer buffer) وهي عبارة عن ملفٍ مؤقت على القرص الصلب الخاص بخادم الملفات، ويتم الاحتفاظ بهذه البيانات إلـــى أن يتـــم إرســـالها للطابعة، فإن كانت الطابعة مشغولة فيتم وضع البيانات المطلوب طباعتها في طابور الانتظار (Queue) إلى أن تفرغ الطابعة.



شكل رقم (١٤-٦) استخدام طابعة مشتركة

٣) البرنامج المساند للدخول (Login utility):

وهو البرنامج الذي يتولى معالجة إجراءات الدخول إلى بيئة الشبكة حيث يحتاج المستخدم إلى اسم وكلمة مرور حتى يمكن حماية البيانات من الاستخدام غير المخول، وبعض نظم التشغيل لا تطلب كلمة مرور للدخول إلى الشبكة فالشبكة مفتوحة طول الوقت، ولكن الوصول إلى بعض الملفات أو البرامج المعينة يحتاج إلى كلمة مرور.

٤) **البرنامج المساند للفهارس (Directeory specification utility):**

وهو أسلوب مشابه لنظام كلمات المرور بهدف حماية الفهارس فهنا تكون الصلاحيات للملفات وليس للمستفيد. فتتاح قراءة "**الملفات العمومية**" (Public Files) للجميع بينما "**الملفات الخاصة**" (Private Files) فلا يمكن الوصول إلى الفهارس الخاصة بها (Directories) إلا لمن له الصلاحيات المناسبة. وينظم هذا البرنامج المساند الدخول إلى "**الفهارس المشتركة**" (Sharable) التي يمكن استخدامها آنيًا من قبل عدة مستخدمين، كما ينظم الدخول إلى "**الفهارس غير المشتركة**" (Non Sharable) التي لا يمكن الدخول إليها من قبل أكثر من مستخدم في الوقت الواحد.

٥) **البرنامج المساند للإغلاق (Locking utility):**

وهو برنامج مساند يتولى حظر استخدام الملف أو السجل أو الحقل لصالح مستخدم معين دون غيره حتى ينتهي من عمله، فعندما يطلب أحد المستخدمين الكتابة على ملف معين يقوم البرنامج المساند **بإغلاق** ذلك الملف حتى تتم التغييرات المطلوبة ثم **يفتح** هذا الملف مرة أخرى أي يتيحه للاستخدام من قبل المستخدمين الآخرين.

٤-٤ الوسائل المادية لتأمين الشبكة المحلية

١) **الأقفال الإلكترونية:**

تستخدم الأقفال الإلكترونية للأبواب والحراسة العادية.

٢) **أقفال الحاسبات الشخصية الحديثة:**

تسمح هذه الأقفال للمحطة الطرفية بالبقاء على الخط ضمن الشبكة (Online) حتى لا تتعطل الشبكة، ولكن مع إيقاف عمل كل من الشاشة ولوحة المفاتيح لمنع استمرار هذه الطرفية في العمل.

٣) نظم الإنذار الآلية:

تدق نظم الإنذار الآلية التي يتم تركيبها على الأبواب والنوافذ أجراس تنبيه عند محاولات الاستخدام غير المرخصة في غير مواعيد العمل.

٤) إلغاء وحدات إدارة الأقراص المرنة:

يتم في كثير من الأحيان اللجوء إلى استخدام حاسبات شخصية لا تحتوي على وحدات إدارة أقراص مرنة بهدف التغلب على المحاولات غير المشروعة لاستنساخ البيانات.

٥) الحماية ضد الإشعاع الثانوي للكابلات:

ويتم ذلك عن طريق عدة وسائل منها :

- وضع "الكابلات" في أماكن محمية غير معرضة لوصول غير المختصين.
- استخدام "الكابل" المغلف بواسطة أسطوانة مضفرة بسلك نحاسي لتقليل الإشعاع الثانوي الصادر عن "الكابل"، ويمكن إضافة أكثر من طبقة (غلاف) للكابل لمنع الإشعاع نهائيًا.
- استخدام "كابلات" الألياف الضوئية (Fiber-Optic cables) التي تلغي نهائيًا عملية الإشعاع الثانوي للكوابل.

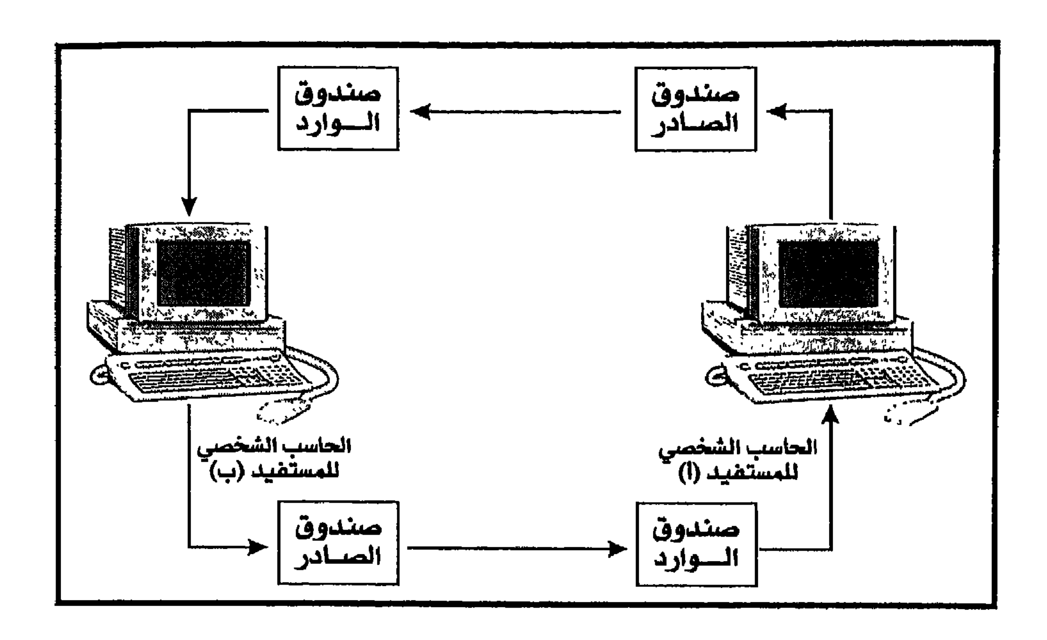
٥- أمن البريد الإلكتروني الداخلي في شبكات "إنترانت"

البريد الإلكتروني هو وسيلة الاتصال بين المستخدمين المشتركين في الشبكة الداخلية "إنترانت" بما يشبه الرسالة التي نتركها على مسجل الهاتف عند عدم وجود الطرف الآخر وقت الاتصال. وهناك عدة وسائل تستخدم لتأمين البريد الإلكتروني نذكر منها:

١) يستخدم لتأمين البريد الإلكتروني أسلوب كلمات المرور بحيث يستطيع المستخدم من أي مكان بالشبكة إرسال أو استلام الرسائل الشخصية، مادام عند دخوله إلى الشبكة قد أعطى كلمة المرور الصحيحة. وبالتالي لا يستطيع غير المصرح لهم بالاطلاع على البريد الشخصي الخاص بالآخرين أو إرسال الرسائل لهم، كما لا يسمح للآخرين بالاطلاع على البريد الصادر من أي مستخدم.

٢) من وسائل التأمين كذلك أن يتم تسجيل اسم المرسل مع كل رسالة ووقت إرسالها والطرفية التي تم منها الإرسال، ويعتبر ذلك نوعًا من التوقيع (Signature) من المرسل على رسالته.

٣) يخصص نظام البريد الإلكتروني منطقة مشتركة على القرص الصلب تستخدم كمركز لحفظ الرسائل، وتسمى (مركز البريد Post Office). وبهذه المنطقة صندوقان لكل مستخدم: أحدهما للإدخال والآخر للإخراج. وعند إرسال الرسالة يتم الربط بين صندوق الإخراج الخاص بالمرسل وصندوق الإدخال الخاص بالمرسل إليه. وبعد الإرسال يتم إخطار المرسل إليه بأن هناك رسالة في صندوق البريد الخاص به، وعند استلام المرسل إليه الرسالة يتم إخطار المرسل بنجاح التوزيع.



شكل رقم (١٤-٧) صناديق بريد المستخدمين

٤) عند إرسال نفس الرسالة إلى عدة مستخدمين، يتم إعداد نسخة من الرسالة في صندوق الإدخال الخاص بكل مستخدم، ولكن في حالة الرسائل الكبيرة تلجأ بعض النظم، بدلاً من تكرار نسخ الرسالة، إلى إرسال إخطار لكل مستخدم بأن هناك ملفًا (مع ذكر اسمه) مرسلاً إليه ويطلب منه قراءة الملف. وفي هذه الحالة لضمان وصول الرسالة لا يمكن محو الملف إلا إذا تم الاطلاع عليه من جانب جميع المستخدمين المرسل إليهم هذا الملف.

٥) لتسهيل الاطلاع على الرسائل أو حذفها أو تأمينها بمستوى معين من الأمن، تقوم بعض نظم البريد الإلكتروني بتصنيف الرسائل بذكر نوع البريد لكل رسالة، فتكون لدينا أنواع متعددة من الرسائل (RPRT أو DOC أو MEMO أو PERSONAL أو GRAPH) إلى جانب البيانات الأساسية مثل: التاريخ والمصدر والعنوان، وبذلك يمكن وضع درجات حماية مختلفة أو مستويات تشارك مختلفة لكل نوع من هذه الأنواع.

٦) في بعض نظم البريد الإلكتروني، وبناءً على رغبة المرسل، يتم تشفير الرسائل المرسلة خلال مرورها بالشبكة.

٧) تقوم بعض النظم كذلك بتشفير الرسائل المخزنة في صندوق بريد المرسل إليه الذي يحدد ذلك مسبقًا بأن يطلب تشفير جميع الرسائل المخزنة في صندوق بريده.

٨) كإجراءٍ احتياطي لعدم ضياع الرسائل المهمة لأي سببٍ من الأسباب يتم في بعض النظم إرسال نسخة من البريد الإلكتروني آليًا على صورة رسالة "فاكسيميلي" للشخص أو الأشخاص المرسلة إليهم الرسالة.

وسنتحدث عن أمن البريد الإلكتروني في شبكة إنترنت العالمية في الفصل الخامس عشر: (أمن شبكة المعلومات العالمية "إنترنت").



الفصل الخامس عشر

أمن شبكة المعلومات العالمية (إنترنت)

موضوعات الفصل:

(١) التعريف بشبكة إنترنت العالمية.
(٢) المشاكل التي تكتنف شبكة إنترنت.
(٣) المخاطر الأمنية على المستوى العالمي.
(٤) المخاطر الأمنية على المستوى العربي.
(٥) شبكة "إنترنت ٢" ومستقبلها.
(٦) تقنيات حماية المعلومات.
(٧) وسائل الحماية في شبكة إنترنت.
(٨) جدران الحماية ما لها وما عليها.
(٩) شبكة "إنترنت" في المملكة العربية السعودية.
(١٠) دور الأجهزة السعودية المعنية بأمن المعلومات في ضمان أمن الشبكة.



نخصص هذا الفصل لدراسة أخطر ما أخرجته التقنية على أمن المعلومات، ونعني به شبكة المعلومات العالمية "إنترنت" التي أصبح لها من الانتشار ومن الفوائد الكثيرة ما يجعلنا لا نستطيع الاستغناء عنها مهما كانت خطورتها على أمن معلوماتنا. ولكن لابد من أخذ الاحتياطات اللازمة وإجراءات الأمن الضرورية في مواجهة النوعية الجديدة من المخاطر التي نشأت مع هذه الشبكة وبسببها. نبدأ الفصل بالتعريف بشبكة "إنترنت" واستخداماتها العديدة ، ثم نتحدث عن المشاكل التي تكتنف الشبكة، والمخاطر الأمنية العديدة على المستوى العالمي وعلى المستوى العربي، نقدم بعد ذلك شبكة "إنترنت ٢" ونتحدث عن مستقبلها.

نتحدث بعد ذلك عن تقنيات حماية المعلومات على الشبكة، ونركز على تقنيات جدران الحماية.

نختتم الفصل بقسمين خاصين بالمملكة العربية السعودية نناقش فيهما بإيجاز تنظيم استخدام الشبكة في المملكة، والمخاطر الأمنية على مستوى المملكة، ودور الأجهزة السعودية المعنية بأمن المعلومات في ضمان أمن الشبكة.

١- التعريف بشبكة إنترنت العالمية

١-١ شبكة إنترنت

شبكة الإنترنت هي مجموعة من شبكات المعلومات الدولية التي ترتبط ببعضها، مما يتيح تبادل المعلومات بين البشر على اتساع العالم كله. وقد أدى التوسع الهائل في استخدام هذه الشبكة في العالم خلال العقد الأخير من القرن العشرين إلى مزيد من الإمكانات الهائلة والفرص المتاحة في مجال البحث العلمي ومجال التجارة والسياحة. وهناك العديد من الخدمات التي يستطيع مستخدمو الشبكة الحصول عليها مثل: خدمات إرسال واستقبال البريد الإلكتروني والمشاركة في (قوائم الاهتمام Mailing Lists) إلى جانب

العديد من الخدمات التي تعتمد على الاتصال الفوري أو التفاعلي (Interactive) ، نذكر منها (موزايك MOSAIC) و(جوفر GOPHER) وخدمة نقل الملفات (FTP) و(تلنت TELNET) أو (بروتوكول محاكاة الطرفية Terminal Emulation Protocol).

ولكن صاحبت هذه التطورات كلها ثغرات أمنية هائلة بحجم الفوائد الجمة التي جنتها البشرية من هذه التقنية الرائعة.

١-٢- استخدامات الشبكة

وفيما يلي عرض لبعض الخدمات التي تقدمها شبكة إنترنت:

١-٢-١- البريد الإلكتروني (Electronic Mail)

ونقصد به الرسائل التي يتم إرسالها من شخص إلى آخر عبر الشبكة، وهي وسيلة اتصال على درجة عالية من الكفاءة للاتصال بالآخرين وعقد الصفقات والاستفسار عن المعلومات من أي مكان على الأرض خلال ثوان معدودة، وربما تفوقت هذه الوسيلة على المحادثة الهاتفية في تجاوز عقبة اللهجات المختلفة، فاللغة الإنجليزية التي تسود معظم مراسلات الشبكة تستخدم مقروءة وليست منطوقة.

١-٢-٢- التجارة الإلكترونية (Electronic Commerce)

تستخدم شبكة إنترنت في عقد الصفقات التجارية إلكترونيًا عن طريق قيام الشركات بإعداد (صفحات خاصة Home Pages) في مواقعها على الشبكة يمكن الدخول إليها والاطلاع على البضائع أو الخدمات التي تقدمها هذه الشركة. ويستطيع راغب الشراء تعبئة نموذج معين وإرساله إلى الشركة (إلكترونيًا) لشحن البضاعة المطلوبة إليه، كما يمكنه كذلك إدراج رقم بطاقة الائتمان الخاصة به ("فيزا" أو "ماستر كارد" مثلاً) لخصم المبالغ المستحقة مباشرة من حسابه المصرفي، ولا يخفى علينا حجم المخاطرة الواردة إذا وقع رقم بطاقة الائتمان في يد طرف ثالث.

١-٢-٣- نقل الملفات (File Transfer Protocol FTP)

يمكن عن طريق الشبكة أيضًا نقل الملفات باستخدام (**بروتوكول نقل الملفات File Transfer Protocol FTP**) وعن طريق هذه الوسيلة يمكن للمستفيد جلب بعض الملفات من مواقع مختلفة على الشبكة إلى حاسبه الشخصي أو العكس بإرسال بعض الملفات إلى جهات أخرى على الشبكة، ويتم ذلك بنفس الأسلوب الذي كان يتم به تبادل الملفات من خلال (لوحات الإعلانات الإلكترونية Bulletin Boards BBS) ، ويمكن الحصول على الملفات المطلوبة بسهولة، إذ يكفي أن يعرف المستفيد أن هناك برنامجًا باسم (Secure) مثلاً وأن هذا البرنامج موجود على الحاسب الخاص بجامعة "أوت باك" في استراليا على سبيل المثال. فباستخدام أمر بسيط يمكن جلب هذا البرنامج إلى القرص الصلب في الحاسب الشخصي للمستفيد خلال دقائق قليلة، يتم ذلك عن طريق الاتصال بين حاسب المستفيد (FTP Client) والحاسب الخاص بالجامعة (FTP Server) عن طريق الأمر:

>ftp outback.edu.au

وعلى الفور يتم توصيل المستفيد بحاسب الجامعة في استراليا، ثم يطلب النظام هناك من المستفيد إدخال الاسم وكلمة السر إذا كان ينتمي إلى الجامعة، أما المستفيد العادي (الذي لا ينتمي إلى الجامعة) فيمكنه أن يدخل اسمًا عامًا هو (Anonymous) ثم يدخل مكان كلمة السر عنوان البريد الإلكتروني الخاص به. وهنا يستطيع المستفيد طلب البرنامج بأن يدخل الأمر التالي:

>get secure.com

ثم ينهي الجلسة ويخرج بإدخال الأمر:

>quit

ولن تمضي دقائق قليلة حتى يصل إليه الملف المطلوب.

١-٢-٤- البحث عن الملفات "آرشي" (Archie)

في المثال السابق كنا نعرف بدقة اسم الملف المطلوب وأين يقع. ولكن الأمر عادة لا يكون بهذه السهولة، فكيف يستطيع المستفيد أن يعرف بوجود ملف معين وبمكان وجود هذا الملف؟ يتم ذلك باستخدام (خادم آرشي Archie server) وهو عبارة عن أداة بحث آلية تساعد مستخدمي الشبكة على الوصول إلى المكان الذي تخزن فيه الملفات التي يريدونها، ويمكن استخدام هذه الأداة من خلال البريد الإلكتروني أو من خلال خدمة (تلنت Telnet) أو عن طريق (الشبكة العنكبوتية WWW). فللوصول مثلاً إلى مكان برنامج كشف الفيروسات Scan يمكن إدخال الأمر التالي:

>archie -s scan

وعند ذلك سوف يقوم آرشي بالبحث عن الملفات التي تحتوي على كلمة (scan) ضمن اسم الملف (سواء بالحروف الكبيرة أو الصغيرة، بسبب استخدام المعامل s- في الأمر)، وفي النهاية يخرج البرنامج نتيجة البحث بالاسم الكامل للملف المطلوب والمكان الموجود به (FTP site)، ومن ثم يمكن الحصول على نسخة من هذا الملف بواسطة (بروتوكول نقل الملفات FTP).

١-٢-٥- التنقيب في شبكة إنترنت "جوفر" (Gopher)

يمكن أن **يجوس** المستفيد خلال شبكة إنترنت عن طريق استخدام (**جوفر Gopher**) وهذا الأسلوب عبارة عن وسيط سهل الاستخدام ويعتمد على القوائم المنسدلة ، ويعرف "جوفر" طريقه خلال الشبكة بفضل العديد من المتطوعين الذين يقضون وقتاً طويلاً في إنشاء (**المؤشرات Pointers**) التي تنتقل بك إلى "المواقع" المفيدة على الشبكة، فبمجرد زيارة أحد مواقع "جوفر" يستطيع المستفيد "**الإبحار**" إلى سلسلة من المواقع الأخرى من خلال مجموعة

من القوائم المتفرعة (**كالشجرة**) حتى يصل إلى الموقع المطلوب . وهناك إما أن يقوم بالإطلاع على المعلومات المخزنة بهذا الموقع، أو ربما يطلب نسخها مثلاً. ويتطلب ذلك وجود برنامج (Gopher Client) على الحاسب الخاص بالمستفيد ومعرفة أحد مواقع "جوفر" لبدء الرحلة منه.

١-٢-٦- البحث عن الملفات "فيرونيكا" (Veronica)

رأينا من قبل كيف أن نظام "**آرشي**" يسهل الحصول على فهرس بالمواقع التي يمكن منها الحصول على الملفات (FTP Sites)، وبالمثل فنظام (**فيرونيكا Veronica**) يمكن من خلاله الحصول على فهرس بمواقع "**جوفر**". وهذا النظام لا يحتاج إلى أي برامج لاستخدامه، فبمجرد الاتصال بأي موقع من مواقع "فيرونيكا" يستطيع المستفيد أن يدخل ما يود البحث عنه، وسيدخل مع النظام في حوار للوصول إلى موضوعات "جوفر" التي تلبي احتياجه. ويمكن للمستفيد الحصول على ما يريد بالاتصال بأي موقع من مواقع "فيرونيكا" فهي جميعًا متشابهة.

١-٢-٧- قوائم الاهتمام (Mailing Lists)

قوائم الاهتمام الهدف منها إعلام المشتركين فيها بآخر التطورات في موضوع معين، وهناك آلاف القوائم يختص كل منها بموضوع معين مثل: سيارات السباق أو الذهاب إلى المريخ أو زراعة الورود أو تربية الأطفال أو مرض السكر أو "وندوز ٢٠٠٠" وهكذا. ويمكن للمستفيد الاشتراك في أي عدد من هذه القوائم، ويتبادل المشتركون في القائمة البريد الإلكتروني للتعريف بآخر مستجدات الموضوع. وباشتراك المستفيد في قائمة معينة تصل إليه نسخة من أي بريد يتم إرساله إلى القائمة وبذلك يظل على صلة بالموضوع الذي يهتم به باستمرار. ويمكن الاشتراك في أي عدد من القوائم،

وهناك بعض القوائم "الساخنة" التي يزداد فيها معدل ورود البريد بشكل كبير. وفي هذه الحالة يستطيع المستفيد أن يخطر القائمة برغبته في تجميع البريد وإرساله إليه مرة واحدة في اليوم مثلاً (Archive) حتى لا يتم إغراقه بالرسائل.

ولمعرفة القوائم الموجودة حاليًا في مجال الأمن يمكن توجيه الأمر:

List global /security

مثلاً لأي عنوان مركزي مثل **listserv@kacst.edu.sa** فتحصل على قائمة بجميع قوائم الاهتمام لتختار من بينها.

ويمكن الانضمام إلى أي قائمة بإرسال طلب اشتراك إلى موقعها، فللاشتراك في قائمة "أمن المعلومات" (infsec-l) نرسل إلى العنوان الذي يستضيف هذه القائمة أو إلى العنوان المركزي Listserv@listserv.net رسالة محتواها:

subscribe infsec-l Hassan Taher

أما إذا أراد المستفيد إخفاء اسمه فيمكنه كتابة أمر المشاركة على النحو التالي:

subscribe infsec-l anonymous

ولإلغاء المشاركة في القائمة يمكن للمستفيد أن يرسل أمرًا بإلغاء المشاركة على النحو التالي:

unsubscribe infsec-l

١-٢-٨- مقهى الإنترنت "يوزنت" (Usenet)

فكرة نظام (يوزنت Usenet) هي فكرة المقهى حيث يجتمع الناس ليتحدثوا ولكي يمارسوا البيع والشراء، أي أنه يكاد يكون مؤتمرًا عالميًا

مكونًا من مجموعات فرعية يناقش كل منها موضوعًا بعينه، وتسمى هذه المجموعات (المجموعات الإخبارية News groups) ويمكن عند الدخول إليها الاطلاع على الرسائل المتبادلة بين المهتمين بهذا الموضوع، ولذلك ينتقي مستخدم الشبكة بعض الموضوعات التي تناقش مجالات اهتمامه لينضم إليها.

ويوجد أكثر من ١٥ ألف مجموعة إخبارية [Rankin-1996] تغطي موضوعات شتى، وهي موزعة على آلاف الحاسبات حول العالم، وعادة يشرف على كل "مقهى" مدير لتنظيم الاستفادة منه. ورغم أن "يوزنت" من الناحية النظرية لا يمكن اعتبار أنها هي شبكة إنترنت إلا أنها عمليًا أصبحت جزءًا لا يتجزأ من أنشطة الشبكة. ويلزم لزيارة المقهى استخدام برنامج (قارئ النشرة Newsreader)، والمقهى يختلف عن قوائم الاهتمام في عدة أمور، أولها: هو أن مقهى إنترنت (يوزنت) هو مكان يذهب إليه المستفيد بينما قوائم الاهتمام هي التي تأتي إلى المستفيد، وثانيها: هو أن المستفيد لا يشترك في عضوية المقهى وإنما يزوره من وقت إلى آخر، أما الاختلاف الثالث فمؤداه أن المستفيد عندما يتراسل مع قوائم الاهتمام يعلم بأن هناك عددًا محددًا من الأشخاص (أعضاء القائمة) هم الذين سوف يتلقون رسالته بينما المستفيد في حالة المقهى لا يعلم من الذين سوف يزورون المقهى أو ما هو عددهم، ولذلك يعرف "بوب رانكين" يوزنت بأنها "حفل مستمر لا ينتهي مقام في غرفة يؤمها العديد من المدعوين غير المرئيين، وهؤلاء المدعوون يكتبون ما يشاءون على حوائط هذه الغرفة ثم يغادرون" [Rankin 1996].

وتندرج المجموعات الإخبارية تحت أحد المجالات السبعة المبينة في جدول رقم (١٥-١).

المجال	الرمز (المقطع الأول)	مثال
قطاع الأعمال	biz	biz.marketplace.international
الحاسب	comp	comp.unix.admin
أمور متنوعة	misc	misc.books.technical
تسلية	rec	rec.pets.dogs.health
قضايا اجتماعية	soc	soc.singles
مناقشات علمية	sci	sci.astro.amateur
دردشة	talk	talk.bizarre

١-٢-٩- "الشبكة العنكبوتية" (World Wide Web WWW)

"الشبكة العنكبوتية" (أو"الويب" كما يطلق عليها) أصبحت الآن أهم أدوات إنترنت لتخزين المعلومات وعرضها والبحث عنها، وتعتمد الشبكة العنكبوتية على البنية التحتية الثرية لشبكة إنترنت، وهي تتكون من العديد من البيانات إلى جانب أدوات الإبحار خلال الشبكة للحصول على هذه البيانات. ويمكن للمستفيد أن يتنقل بين الوثائق والمواقع المختلفة على الشبكة عن طريق النقر على بعض الكلمات أو الصور على شاشة الحاسب، حيث يتم نقله أو (وصله) بموقع آخر يتحدث بتفصيل أكثر عن هذه الكلمة أو الصورة، وفي الموقع الجديد ربما يود المستفيد الانتقال إلى مواقع أخرى، وهكذا يظل يتشعب لدرجة أن بعض المستفيدين قد ينسى الموضوع الأصلي الذي بدأ به قبل أن يأتي إلى المكان الذي وصل إليه، ومن هنا جاءت تسمية "الشبكة العنكبوتية".

ومن المزايا الرائعة لصفحات (الويب Web pages) أنـــها تحتـــوي، بالإضافة إلى النصوص العادية، على الصور والأحاديث المسجلة والموسيقى والصور المتحركة (الفيديو)، ويمكن للمستفيد استخدام (**متصفـــح Browser**) لعرض صفحات "الويب" ولمساعدته في الإبحار خلال الشـــبكة فـــي رحلـــة ممتعة على خلفية رائعة من "الملتيميديا". ومن أشهر (**الـــبرامج المتصفحـــة Browsers**) برنامج (**نتســـكيب Netscape**) ونظـــيره العربـــي "**ســـندباد**" بالإضافة إلى بعض البرامج المتصفحة الأخرى الأقل شهرة مثل (**موزايـــك Mosaic**) و(**مستكشف إنترنت Internet Browser**)، كمـــا أن الشـــركات التي تقدم خدمة إنترنت للمســـتفيدين (Internet Service Providers ISPs) مثل هؤلاء الفرسان الثلاثة الذين يحصلون على نصيب الأسد مـــن الســـوق العالمية ("أمريكا أون لاين" و"كمبيوسيرف" و"بروديجي")، هـــذه الشـــركات لديها برامجها المتصفحة الخاصة بها والتي يستطيع المشـــترك جلبـــها مـــن الشبكة واستخدامها للتجول خلال الشبكة العنكبوتية. وتستضيف الشبكة أكـــثر من ٢٥ مليون موقـــع [Rankin 1996] أنشـــأتها الجامعـــات والمنظمـــات والشركات بل والأفراد العاديون. ومن خلال الشبكة يمكن للمستفيد التســـوق من بعض المحلات مثلاً، أو إرسال بطاقة تهنئة لصديق، أو مســـح جميـــع معارض السيارات للوصول إلى أفضل ســـعر لشـــراء ســـيارة جديـــدة، أو الاستعلام عن أسعار الأسهم، أو الحصول علـــى دورة تدريبيـــة بأســـلوب الاتصال المباشر، أو إجراء بعض المكالمات الهاتفيـــة الدوليـــة، أو ربمـــا مشاهدة فيلم سينمائي، أو التجول في معرض فني، أو إجراء بحث فـــي أي موضوع يمكن تخيله، أي باختصار شديد **كل شيء**.

لكل صفحة (أو موقع على الشبكة) عنوان، وهذا العنوان يسمى في لغة الشبكة (Uniform Resource Locator URL) وهو يحدد للبرنامج المتصفح الاسم والموقع وأسلوب جلب وعرض هذه الصفحة، وتتكون هذه العنـــاوين عادة من ثلاثة مقاطع: اسم البروتوكول المستخدم، واسم الحاسب المضيـــف

(Host) ، واسم الملف. وفيما يلي مثال لأحد العناوين:

http://www.sample.com/welcome.html

فالبروتوكول المستخدم هنا هو (http) والحاسب المستضيف هو (www.sample.com) والملف اسمه (welcome.html) .

وتسمح الشركات مقدمة الخدمة (ISP) في الغالب للمشتركين بإنشاء مواقعهم الخاصة بهم (Home Pages) على الشبكة حيث يمكن أن يعرف المستفيد نفسه أو شركته للعالم، ويمكن تنفيذ ذلك باستخدام لغة (HTML) وهي لغة لمعالجة النصوص تستخدم بعض الرموز لوصف عناصر الوثيقة المطلوب إعدادها كما تحدد للبرنامج المتصفح كيفية عرض الوثيقة على شاشة الحاسب.

١-٢-١٠- "الإصبع" (Finger)

(الإصبع Finger) هي أداة بسيطة يمكنها أن تعطي المستفيد المعلومات المطلوبة عن أي مستفيد آخر على الشبكة، وقد استعارت هذا الاسم من كونها تشير إلى المستفيد المطلوب كما يشير الإصبع، ويلزم لاستخدام هذه الوسيلة أن يكون لدى المستفيد عنوان البريد الإلكتروني للشخص المطلوب مثل:

daoudh@ipa.edu.sa

وعند البحث عن مستفيد يتم إرسال طلب إلى الحاسب الذي يتبعه هذا المستفيد للحصول على جميع المعلومات المخزنة لديه عن هذا المستفيد (في حدود المصرح به طبعًا)، وتختلف الإجابة التي يتم الحصول عليها كثيرًا من نظام إلى آخر وفقًا لقواعد الخصوصية المتبعة، ولكن الحد الأدنى من المعلومات الذي يمكن الحصول عليه هو الاسم ومتى كانت آخر مرة قام فيها هذا المستفيد بالدخول إلى النظام (Login). ويمكن الاستفادة من معرفة آخر

مرة دخل فيها المستفيد إلى النظام في معرفة ما إذا كان هذا المستفيد قد قرأ الرسالة التي تم إرسالها إليه منذ يومين مثلاً أم لا.

١-٢-١١- "تلنت" (TELNET)

خدمة (تلنت Telnet) تتيح للمستفيد استخدام حاسب آخر عن طريق شبكة إنترنت، ربما للحصول على بعض المعلومات المفيدة المخزنة في قاعدة بيانات هذا الحاسب، أو حتى تنفيذ بعض البرامج عليه. واستخدام هذه الوسيلة يختلف عن الوسائل السابقة فهو يجعل المستفيد (**ينتقل**) إلى الحاسب الآخر ويدخل إليه ويستخدمه كما لو كان موجوداً في ذلك الموقع البعيد. أما استخدام "الشبكة العنكبوتية" فلا يتعدى قيام "المتصفح" بإرسال استعلامات إلى الحاسبات الأخرى ويتلقى ردودها في صورة صفحات من المعلومات دون الانتقال الفعلي.

وجدير بالذكر أن خدمة "تلنت" مقصورة على النصوص فليست هناك أزرار للنقر عليها أو صور للإشارة إليها. وعند استخدام هذه الخدمة تقوم البرمجية الخاصة بها (**بمحاكاة الشاشة**) المتصلة بالحاسب الآخر **(Terminal Emulation)**، ومعظم أنواع الشاشات في شبكة إنترنت من النوع (VT100) فيما عدا قلة بسيطة.

أما بالنسبة للوحات الإلكترونية التي تعمل بنظام "دوس" فهي عادة تستخدم النوع (ANSI) بينما حاسبات "آي. بي. إم" الكبيرة فهي تستخدم النوع (TN3270).

وحتى يتمكن المستفيد من الدخول إلى حاسب آخر فعليه بالطبع أن يعرف عنوان ذلك الحاسب (وأحيانًا قد يلزم أيضًا معرفة رقم "المنفذ" (Port) على هذا الحاسب) وعند الاتصال يطلب الحاسب من المتصل إدخال رقم المستفيد وكلمة السر ليسمح له بالدخول والاستفادة من خدمات هذا الحاسب.

ويتعين على المستفيد بعد الدخول استخدام أوامر نظام التشغيل الخاص بذلك الحاسب سواء كان "دوس" أو "يونيكس" أو "في إم" مثلاً.

١-٢-١٢- "المحادثة" (Internet Relay Chat IRC)

يمكن التخاطب مباشرة مع المستفيدين الآخرين على الشبكة في أي مكان في العالم باستخدام نظام "**المحادثة**" (IRC) وذلك عن طريق إرسال واستقبال رسائل قصيرة وتبادلها مع الآخرين. ولاستخدام هذه الوسيلة يلزم أن يحصل المستفيد على برمجية (IRC Client) والتي تربطه مع (IRC Server) وهو حاسب آخر يقوم بدور الوسيط في المحادثة، ويمكن جلب هذا البرنامج بسهولة من الشبكة عن طريق وسيلة (FTP) إن لم يكن موجوداً لدى المستفيد.

وقد نال هذا الأسلوب من الاتصال شهرة عريضة خلال حرب الخليج الثانية عام ١٩٩١م وكذلك خلال محاولة الانقلاب الفاشلة على الرئيس الروسي "بوريس يلتسين" عام ١٩٩٣م، وأخيرًا خلال غارات حلف شمال الأطلنطي على كوسوفا عام ١٩٩٩م، حيث كان المراسلون الصحفيون وغيرهم يقومون بإرسال آخر الأنباء مباشرة إلى شبكة إنترنت والإجابة عن الاستفسارات المختلفة مباشرة من قلب الأحداث باستخدام أسلوب (IRC)، وربما ـ هنا فقط ـ تيقن الجميع أن العالم قد دخل بالفعل (عصر الحاسب).

١-٢-١٣- البحث عن مستخدمي الشبكة (Whois)

برغم عدم وجود (**دليل**) للبشر في عالم إنترنت ، فإنه يمكن البحث عن الأصدقاء القدامى مثلاً عن طريق بعض الأدوات المفيدة التي يمكنها العثور على عناوين الأشخاص الذين يبحث عنهم المستفيد . ومن هذه الأدوات خدمة (WHOIS) والتي تقوم بالبحث في قاعدة بيانات ضخمة لمستخدمي إنترنت، ويمكن استخدامها في البحث عن الأشخاص أو الشركات أو عن المكان الذي

يوجد فيه موقع معين على الشبكة ، وذلك عن طريق إرسال رسالة إلى العنوان (mailserv@internic.net) تحتوي على السؤال (whois pc magazine) مثلاً أو (whois Hassan Taher).
وهناك مواقع يمكن اللجوء إليها للبحث مثل (http://www.lookup.com) أو (http://www.whowhere.com) حيث يتم الدخول إلى الموقع ثم استخدام الأمر (Find People) أو الأمر (Find Business) للوصول إلى الشخص أو الشركة المطلوبة.

٢- المشاكل التي تكتنف شبكة إنترنت

٢-١- هموم في ملف إنترنت

مشكلة الأمن تزداد حدة في الشبكات عنها في أجهزة الحاسب المستقلة غير المرتبطة بالشبكات، ففي هذا النوع من الأجهزة المستقلة تقبع بيانات المستفيد في جهازه محصنة داخل صالة التشغيل، ويستطيع المستفيد أن يتخذ ما يشاء من إجراءات الأمن المادية لتأمين غرفة الحاسب ثم ينام قرير العين، ولكن مع وجود الشبكات التي أصبحت تربط الحاسبات في العالم كله فالأمر يختلف، إذ أصبح الحاسب الموجود في المؤسسة يستقبل ويرسل مئات وآلاف الرسائل يوميًا إلى كل مكان وأي مكان، بل إن الآخرين، علاوة على ذلك، يستطيعون تشغيل برامجهم على جهاز الحاسب الخاص بالمؤسسة عن بعد دون سيطرة من المسئولين عنها على ذلك.

هذه التطورات التي يراها كثير من المتخصصين إيجابية قد خلقت مشاكل أمنية جانبية، إذ زادت من الهواجس الأمنية لدى المؤسسات التي ترتبط حاسباتها بالشبكات العالمية، بل لقد بدأ المستفيدون في الجهات ذات الصبغة الأمنية الحساسة يخشون على بياناتهم من أن تتسرب من بين أيديهم

بعد أن زادت المخاطر التي تكتنف البيانات في عصر الشبكات، فكثير من الجهات تتصل بفروعها عن طريق الهاتف أو عن طريق أطباق "الميكروويف"، وفي كلا الحالين تمر البيانات برحلة محفوفة بالمخاطر، وتكون البيانات خلال هذه الرحلة غير الآمنة عرضة للاختراق إما بالاطلاع عليها أو بتعديلها.

٢-٢- تصنيف هموم شبكة إنترنت

شبكة إنترنت العالمية لم تبلغ الحلم بعد، وفي بعض البلاد العربية لم تبلغ حتى سن الفطام، بل ربما هي، في بعض البلدان، لم تولد بعد! وبرغم هذه الحقيقة، وبرغم أن شبكة إنترنت تصنف في خانة الحداثة وتعتبر من صرعات آخر الزمان، وبرغم أنها تعتبر التركة العظيمة التي تركها القرن العشرون لوريثه الحادي والعشرين، برغم كل ذلك فإنها تعاني من الكثير من الهموم الأمنية التي قد تهدد مسيرتها.

ربما استطعنا أن نصنف هذه الهموم على مستويات عدة، فبعضها هموم على مستوى العالم، والبعض الآخر على مستوى عالمنا العربي، والبعض الثالث على مستوى المملكة العربية السعودية.

سنبدأ بالحديث عن الهموم العالمية والعربية ونترك مشاكل الشبكة في المملكة العربية السعودية للقسم الأخير من هذا الفصل. وسنركز اهتمامنا عند التصدي لهذه الهموم لما يؤثر في أمن المعلومات أو يتأثر به.

٣- المخاطر الأمنية على المستوى العالمي

على المستوى العالمي نجد أن هموم الشبكة ثلاثة: الأمن والازدحام والمادة المتداولة على الشبكة.

٣-١- مشكلة الأمن

الأمن هو مشكلة صاحبت الشبكة منذ نشأتها، فقد تكاسل مستخدمو الشبكة ومتخصصو الحاسب الآلي طويلاً عن الاهتمام بمشكلة الأمن والكل يظن أن بياناته في مأمن وأن اتصالاته عبر الشبكة مؤمنة تمامًا، وأن قواعد البيانات التي أنفق الملايين على إنشائها ترقد آمنة مطمئنة في أحضان صالة الحاسب الآلي في مؤسسته أو وزارته، وبالتالي فليس ثمة ضرورة لكي يزعج نفسه بمسألة الأمن هذه فهي من قبيل الترف والرفاهية. ولكن الحقيقة غير ذلك ففي كل يوم تطالعنا الأنباء باختراقات هائلة للشبكة تهدد أمن البيانات فيها، ومن ثم أمن أصحاب هذه البيانات.

٣-١-١- أثر التوسع في الاستخدام

وتزداد المشكلة حدة كلما ازداد استخدام الشبكة من جانب المستفيدين، وكلما فتحت التقنيات الحديثة آفاقًا جديدة لاستخدامات هذه الشبكة مثل التسوق الإلكتروني، والذي انتشر في هذه الأيام، حيث يتم التسوق عن طريق إرسال رقم بطاقة "الفيزا" أو "الماستر كارد" عبر الشبكة للشركة مقدمة الخدمة أو الشركة بائعة السلعة . وبالطبع لو أن هذه المعلومات وقعت في يد غير أمينة لأمكن إساءة استغلالها. ومن الآفاق الجديدة كذلك انتشار مفهوم التجارة الإلكترونية ، التي اتسع نطاق استخدامها بشكل كبير هذه الأيام بين الشركات الكبرى ومناطق التوزيع التابعة لها في الدول المختلفة.

بعد كل هذا التوسع في استخدام شبكة إنترنت والأهمية المتزايدة التي يعلقها المستخدمون على هذه الشبكة كوسيلة اتصال لا غنى عنها، أصبح من الأهمية بمكان الاطمئنان الكامل على أمن البريد الإلكتروني المتداول عبر الشبكة، وعلى سلامة بيانات المؤسسة القابعة في قواعد للبيانات متصلة

بالشبكة ومعرضة للدخول إليها من أي مكان في العالم. وهذا الأمن المنشود هو للأسف ما تفتقر إليه شبكة إنترنت، وهذا أيضًا هو ما يتطلب الكثير من اهتمام مستخدمي هذه الشبكة.

٣-١-٢- محاولات الاقتحام لا تتوقف

وقد تناقلت الصحف في أواخر عام ١٩٩٨م نجاح أحد قراصنة المعلومات الألمان (Hackers) في الوصول إلى شبكة المعلومات الخاصة بالبنتاجون (وزارة الدفاع الأمريكية) وتمكنه من الحصول على كلمة السر الخاصة بأحد كبار جنرالات الجيش الأمريكي، وكيف أن هذا الشاب كان بمقدوره التسبب في أضرار كبيرة لولا اكتشاف أمره. وفي مطلع عام ١٩٩٩م أعلنت وكالة المخابرات المركزية الأمريكية عن رصد ٢٥ ألف محاولة للوصول إلى الملفات السرية التابعة لها وأن ٦٥% من هذه المحاولات قد نجح في اختراق خط الدفاع الأول لنظم المعلومات وبعضها قد تمكن من الوصول إلى قواعد البيانات التابعة للوكالة، وذلك وفقًا لمصادر وكالات الأنباء، وعاد المتحدث باسم البنتاجون فخفف من قتامة الصورة بأن ذكر في مارس ١٩٩٩م أن الأمن القومي الأمريكي لم يتعرض للخطر بسبب هذه المحاولات كما بينا في الفصل الثالث عشر من هذا الكتاب (أمن شبكات نقل المعلومات). أما صحيفة "لوفيجارو" الفرنسية فقد ذكرت مؤخرًا أن الحسابات المصرفية التي يُعتقد أنها تعرضت لمحاولات سطو أو على الأقل لعمليات تلصص من خلال الحاسب الآلي أو شبكة إنترنت قد بلغ عددها حوالي ٣٠ مليون حساب مصرفي على مستوى العالم. بينما كشفت الحملات التفتيشية الدورية في الولايات المتحدة عن أن ٨٠ ألف خط تليفوني خاصة بالسياسيين كانت مفتوحة، أو قل مفضوحة، على شبكة إنترنت ومتاحة لقراصنة التلصص والاستماع وسرقة المعلومات، ذلك لأن الكثيرين الآن

يستخدمون شبكة إنترنت لإجراء المكالمات الدولية الطويلة بسعر المكالمة المحلية، ولا يحتاج ذلك إلى أكثر من أن يكون الحاسب الشخصي الخاص بالمستفيد مزودا بميكروفون وسماعات!.

٣-١-٣- اكتشاف الاختراقات الأمنية بالصدفة

الأمر الذي لا يبعث على الاطمئنان هو أن الصدفة البحتة كانت وراء اكتشاف معظم الاختراقات الأمنية نتيجة خطأ من جانب المقتحم وليس بفضل الإجراءات أو الضوابط الأمنية المتبعة، ويزيد الأمر خطورة أن الكثير من هذه الاختراقات قد تحقق باستخدام وسائل بسيطة غير معقدة أو محترفة. ومن المنطقي أن نستنتج أن الاقتحام في المستقبل لن يكون اقتحام هواة أو فضوليين أو مبتدئين، ممن قد لا نخشى جانبهم، ولكن المتوقع أن يتم الاقتحام، ومن ثم إساءة استغلال شبكة إنترنت من جانب المحترفين الذين يستطيعون الاستفادة من المعلومة واستغلالها بشكل إجرامي. والمشكلة الأخطر تكمن في أن المستخدم ربما لن يعرف بتسرب معلوماته فور حدوث ذلك التسرب، فليست هناك أقفال مكسورة أو أبواب محطمة أو ملف مفقود مما يؤدي إلى اكتشاف السرقة أو اكتشاف التخريب، فهي جرائم يصعب اكتشافها في الوقت المناسب، وحتى عند اكتشافها يصعب معرفة المجرم فهو لا يترك وراءه بصمات أصابع أو آثار أقدام.

لكل ذلك فإنه ما لم يتم اتخاذ الإجراءات الأمنية اللازمة (وهي لحسن الحظ سهلة ومعروفة) لتأمين أجهزة الحاسب المرتبطة بالشبكة وقواعد البيانات الموجودة لدى الوزارات والمؤسسات، سواء كانت هذه الجهات من الجهات الأمنية الحساسة أو من غيرها، ما لم يتم ذلك فلابد من فصل المعلومات ذات الطبيعة الحساسة عن باقي الشبكات المرتبطة بالمؤسسة ضمانا لسريتها.

ولا تكف أجهزة الأمن في جميع الدول عن مراقبة محاولات السطو على المعلومات وملاحقة المتسببين فيها، وهذا ما يعطي أهمية فائقة لتقنيات أمن المعلومات وهو مجال من أكثر مجالات تقنية المعلومات أهمية، والذي تزداد أهميته كل يوم ونحن نعبر بوابة القرن الحادي والعشرين حيث سوف يتسارع في هذا القرن ظهور التقنيات الحديثة وتتعاظم الإمكانيات الفنية التي تتيحها هذه التقنيات مما يفتح المجال لثغرات أمنية أكثر خطورة .

ولما كانت تقنيات أمن المعلومات سهلة وميسرة، ولما كان الكثير منها متاحًا في الوقت الحالي لاستخدام الجميع من أفراد ومؤسسات أو أجهزة أمن (باستثناء بعض التقنيات التي لا تسمح الدول الكبرى التي ابتكرتها بأن تطرح للاستخدام العام) فلا عذر لدينا إن نحن لم نتخذ كافة الاحتياطات لتأمين معلوماتنا التي هي أثمن ما تمتلك المؤسسات في عصر المعلومات، ذلك العصر الذي أصبحت فيه المعلومات قادرة على أن تكون هي الفيصل بين النصر والهزيمة في وقت الحروب ، أو أن تكون في وقت السلم هي الفيصل بين التفوق والانكسار.

٣-٢- مشكلة الازدحام

الهم الثاني على المستوى العالمي هو الازدحام؛ فنحن نعرف جميعًا معدل الازدياد الهائل في حجم الشبكة التي تضم إليها في كل يوم شبكات جديدة وحاسبات جديدة ومستخدمين جدد، ومن ثم هناك في كل يوم بريد أكثر يتم تبادله عبر خطوطها، هذه الخطوط التي تتفاوت من ناحية السرعة والكفاءة. فبعض الشبكات في كثير من الدول تنوء بخطوط قليلة السعة وبنية تحتية متهالكة وتقنيات اتصالات قديمة. ولذلك فالازدحام موجود والاختناق حادث والأمر يشبه تدافع السيارات السريعة إلى شارع ضيق مكتظ أصلاً بالسيارات، فتزداد فرص التعطل وفرص عدم وصول الرسائل إلى أهدافها ولذلك أثر كبير على أمن الرسائل المتبادلة عبر الشبكة.

والأمور في هذه النقطة بالذات تسير من سيئ إلى أسوأ على مستوى العالم، ففي الولايات المتحدة مثلاً، وهي أكبر الدول المستخدمة للشبكة، يعاني مستخدمو الشبكة من ازدحام شديد في أوقات الذروة المسائية وبصفة خاصة في مناطق الغرب الأمريكي حيث شبكات الهاتف أقل كفاءة. ويزيد الأمر سوءاً أن المعلومات المتبادلة على الشبكة لم تعد مجرد نصوص كما كان البريد الإلكتروني في الماضي، ولكنها الآن تتجه نحو مزيج متزايد من الصور والصوت والفيديو، وهذه الأشكال من المعلومات من طبيعتها ضخ كميات كبيرة من البيانات عبر الشبكة مما يزيد من مشكلة الازدحام. وهذا الوضع آخذ في التأزم يومًا بعد يوم، وما ينقذ الشبكة حتى الآن هو فارق التوقيت حول الكرة الأرضية الذي يوزع ساعات الذروة على مدار الساعة في العالم!

وعلاج ذلك يتم حاليًا بتحديد كميات البريد الإلكتروني المتبادل ، ولكن هذا من قبيل المسكنات فقط لا غير فالحل الأفضل يكمن في تحسين نوعية شبكات الهاتف في الدول المشتركة في إنترنت، فهذه الشبكات في بعض الدول هي التي تمثل عنق الزجاجة. ومن المتوقع في المستقبل القريب أن يتم منع بعض الدول من الانضمام إلى شبكة إنترنت بسبب تهالك البنية التحتية للاتصالات لديها.

٣-٣- المادة المتداولة

الهم الثالث على المستوى العالمي هو طبيعة المادة المتداولة على الشبكة. فهناك الكثير من القلق الذي يراود المجتمعات المحافظة بسبب ما يتردد حول المواد المنشورة أو المتداولة عبر الشبكة، وضرورة حظر بعض المواد الإباحية أو المواد السياسية غير المرغوب فيها.

٣-٣-١- المواقع على الشبكة

هناك خصوصية فريدة لشبكة إنترنت تجعلها أخطر من القنوات الفضائية التي تملأ الجو من حولنا بذبذباتها وموجاتها "الإلكترومغناطيسية" وتدخل البيوت كاشفة أكثر مما تخفي، فهذه الفضائيات محكومة من الدول أو الشركات التي تهيمن عليها، أما على الشبكة فيستطيع أي شخص فرد أن ينشئ لنفسه موقعًا على الشبكة، وهذا الموقع يستطيع أن يضع عليه ما يشاء من الصور أو الموضوعات أو الآراء السياسية أو التبشير الديني... والمجال مفتوح بلا قيود. ولا نهاية لما يمكن أن يضعه أي شخص أو تضعه أي هيئة أو جماعة على الشبكة. وإذا علمنا أن هذا الموقع يمكن زيارته من جانب آلاف الأشخاص يوميًا نستطيع أن نتصور كيف تنتشر الدعوة التي ما كان لها أن تنتشر بهذه السرعة والكثافة إلا عن هذا الطريق، ومن هنا يتضح حجم المشكلة، التي أصبحت الآن تتعلق بأمن الدول والشعوب وحرية العقيدة الدينية بل وتطول بالتهديد ديننا الحنيف.

٣-٣-٢- سهولة كشف المواقع المشبوهة

ولكن الوصول إلى أصحاب هذه المواقع سهل بعد معرفة عناوينهم، وقد طالعتنا الأنباء في صيف عام ١٩٩٩م بخبر الرجل الذي تم ضبطه في منزله في هونج كونج بعد أن تم رصد تبادله للأفلام الإباحية عبر الشبكة مع شاب آخر في ألمانيا وداهمت الشرطة مسكنه وضبطت عشرات الأفلام الإباحية التي حصل عليها جميعًا عن طريق الشبكة.

٣-٣-٣- ليست كل المعلومات بريئة

حتى المعلومات (البريئة) الموجودة في قواعد المعلومات العالمية يمكن أن يساء استخدامها، وليس بعيدًا عنا كيف أن الشابين اللذين ارتكبا جريمة تفجير المبنى الحكومي في "أوكلاهوما" بالولايات المتحدة عن طريق استخدام

قنبلة محلية الصنع قد حصلا على المعلومات اللازمة لصنع هذه القنبلة عن طريق شبكة إنترنت. فما عليك إلا أن تدخل كلمتي (make+bomb) للبحث حتى تصل إلى مبتغاك.

٣-٣-٤- العلاج

ولعلاج هذه المشكلات فهناك الكثير من البرمجيات المعدة لذلك مثل (جدار الحماية Firewall) الذي يمنع الدخول إلى بعض المواقع، ولكن يجب معرفة هذه المواقع أولاً وتحديد عناوينها حتى يمكن منع الدخول إليها ، ولكن ما يحدث هو أن صاحب الموقع المحظور يمكنه دائمًا أن يرتدي قناعًا آخر، أي أن ينشئ موقعًا جديدًا باسم جديد وهوية جديدة.... وتستمر المطاردة.

يخفف من حدة هذه المشكلة أنه يلزم الإلمام ببعض مبادئ الحاسب الشخصي لمن يريد استخدام الشبكة بعكس القنوات الفضائية التي يمكن للنشء الصغير وبكبسة زر واحدة أن يتجول بين فضائيات متعددة.

٤- المخاطر الأمنية على المستوى العربي

تحدثنا عن بعض الهموم الأمنية التي يمتلئ بها ملف شبكة إنترنت على المستوى العالمي، أما على المستوى العربي، فالعالم العربي ليس بعيدًا عن هذه الهموم العالمية فهو يعاني منها شأنه شأن باقي الدول المشتركة في الشبكة، وهناك بالإضافة إلى هذه الهموم العالمية هموم أخرى خاصة بالمجتمعات العربية، أبرزها همان أساسيان هما: التعريب والتكلفة العالية، وهذه الهموم لها تأثيرها السلبي على أمن المعلومات المتبادلة طالما أنها تؤثر على استخدام العرب للشبكة ونقلهم لمعلوماتهم عبرها ونستعرض هذه الهموم فيما يلي:

٤-١- التعريب

من القيود التي تحد حاليًا من انتشار استخدام الشبكة في العالم العربي هو قيد اللغة ، فلابد لمن يستخدم الشبكة أن يتقن اللغة الإنجليزية. وربما كان ما تقدمه بعض الشركات العربية من خدمات تعريب في هذا المجال لتعريب برامج الاستعراض (Browsers) وبرامج البحث وبرامج النشر على الشبكة وحتى برامج الوقاية من المواد غير المرغوبة، ربما كان هذا العطاء من جانب شركات البرامج العربية يجعل الأمر سهلاً للمستخدم العربي، ويسهل من تبادل المعلومات على الشبكة باللغة العربية ولكن يظل عائق اللغة قائمًا ولا يمكن أن يستغني المستخدم العربي تمامًا عن معرفة اللغة الإنجليزية، حيث إنه حتى الآن ما يزيد عن ٩٥% من المعلومات المنشورة هي معلومات باللغة الإنجليزية. ولعل ذلك يفسر أن استخدام الشبكة في العالم العربي حتى الآن يكاد يكون قاصرًا على الصفوة من المثقفين والمتعلمين ممن يتقنون (لغة الشبكة) إن جاز هذا التعبير.

والتوسع في استخدام البرمجيات العربية الخاصة بالشبكة سيزيد من كمية المادة العربية المنشورة على الشبكة مما يزيد من مستخدميها، وهكذا تدور العجلة.. نفس العجلة التي دارت منذ عشرين عامًا وأدت إلى ظهور الشبكة في نواتها الأولى (أربانت ArpaNet).

٤-٢- التكلفة العالية

أما الهم الثاني على مستوى العالم العربي فهو ارتفاع التكلفة، فحتى الآن توجد تكلفة ملحوظة على المستخدم العادي الذي يريد استخدام الشبكة، فعليه أن يشتري حاسبًا شخصيًا وجهاز "مودم" سريع وبعض البرمجيات مثل: برمجيات الاستعراض وربما برمجيات النشر على الشبكة وغيرها،

وعليه أيضًا أن يشتري النسخ المعربة من هذه البرمجيات. وهذه التكلفة العالية تجعل الأمر صعبًا على بعض الفئات مما يؤخر من انضمام الكثيرين في الدول العربية إلى قافلة مستخدمي هذه الشبكة العالمية، أو بعبارة أخرى قافلة المعجبين بهذه الفاتنة الساحرة إنترنت.

٥- شبكة "إنترنت ٢" ومستقبلها

تحدثنا عن الهموم التي يحفل بها ملف شبكة "إنترنت" العالمية على المستوى العالمي والمستوى العربي والمستوى السعودي. وقد أكملت هذه الشبكة الثلاثين من عمرها الذي أثقلت كاهله المشاكل، وبازدياد هذه المشاكل وتفاقمها بدأ العالم منذ عام ١٩٩٥م يفكر في البديل .. شبكة جديدة شابة فتية تكون هي البديل وتكون هي الأمل.

٥-١- محل ميلاد الشبكة

تزهو ولاية "نورث كارولينا" الواقعة على الساحل الشرقي للولايات المتحدة الأمريكية لا بالملايين السبعة الذين يعيشون فيها ولا بإطلالتها على الطرف الغربي للمحيط الأطلنطي ولكن بأنها أصبحت المهد الذي وُلدت فيه هذه الشبكة الأمل (إنترنت ٢) ، ففي هذه الولاية بدأت الشبكة الوليدة تحبو أولى خطواتها .. نفس الخطوات المترددة الوجلة التي خطتها الشبكة الأم (إنترنت ١) منذ أكثر من ربع قرن.

هذه المولودة الجديدة هي شبكة اتصالات رقمية لنقل وتبادل المعلومات بكافة صورها: النصوص والرسوم البيانية والصور الثابتة والمتحركة والفاكس والصوت والفيديو، أي باختصار كل وسائل التعبير التي يستخدمها البشر في التعامل فيما بينهم، ولذلك جاءت هذه الشبكة فائقة السرعة (٢,٤ جيجا بت).

قد تم الآن تركيب هذه الشبكة بالفعل باعتبارها نواة الجيل الثاني من شبكة إنترنت وبدأت العمل في شهر فبراير ١٩٩٧م، وتربط هذه الشبكة في مرحلتها الأولى الجهات الأكاديمية والحكومية والتجارية في ولاية نورث كارولينا.

٥-٢- المولود العملاق: جيجا نت

جاءت هذه الشبكة كثمرة للتعاون البناء والمثالي الذي أظهره القطاع الخاص والقطاع الحكومي في الولايات المتحدة الأمريكية في بناء البنية الأساسية لهذه الشبكة، وقد شمل هذا التعاون حتى الآن الجهات العاملة في مجالات الصناعة والمجالات التعليمية.

يضم ذلك الجزء من الشبكة الذي كان له شرف البداية كلاً من "مركز تطوير التقنيات" بالولاية (MCNC) وجامعة "ديوك" وجامعة "ولاية نورث كارولينا" وجامعة "نورث كارولينا" في "شابل هيل". ويطلقون على هذه الشبكة الجديدة التي تشكل نواة "إنترنت ٢" اسم "نورث كارولينا جيجا نت" (GegaNet) بسبب كفاءتها العالية.

٥-٣- انسيابية المرور

وقد تم تصميم هذه الشبكة بحيث تقدم لمراكز البحث العلمي والمعاهد التعليمية الجيل القادم من تقنيات ربط الشبكات، تلك التقنيات التي لم تكف عن التطور بشكل درامي خلال العقدين الماضيين ولا تنبئ عن أنها تنوي تغيير هذه السمة في المستقبل المرئي. وسوف تتيح هذه الشبكة الجديدة انسيابية المرور التي كانت تشكو منها سابقتها (إنترنت ١) وذلك عن طريق إيجاد (نقطة تواجد عظيمة القدرة High Capacity Point Of Presence) يمكنها نشر المعلومات في أرجاء الشبكة بكفاءة.

والجزء الحالي الذي بدأ تشغيله تبلغ سرعة نقل المعلومات فيه (٦٢٢) ميجا بت في الثانية، وهو يُستخدم للربط المباشر بين مباني الحرم الجامعي العديدة في الجامعات المرتبطة بالشبكة. وقد بدأ مؤخرًا تنفيذ بعض التطبيقات المشتركة التي تخدم تبادل البيانات بين الكليات المختلفة.

٦- تقنيات حماية المعلومات

على المستوى التقني هناك حلول للعديد من المشكلات الشائعة المرتبطة بشبكة إنترنت، ولكن لسوء الحظ فالأمر هنا لا يختلف عن باقي قطاعات أمن المعلومات ، إذ إن هناك دائمًا محاولة للموازنة بين الأمن وبين تبسيط الإجراءات، فالحماية الفعالة تعتمد على فرض القبول بالسياسة الأمنية الموضوعة وعلى فرض تطبيقها، بالإضافة إلى استخدام الحلول التقنية الحديثة مثل (**البطاقات الذكية Smart Cards**) و"**الاتصالات المشفرة**" و"**البوابات**" (عدم الارتباط المباشر بإنترنت)، وهي كلها تقدم الحل لأنواع مختلفة من المشكلات. ولكن إذا لم يُؤخذ الأفراد بعين الاعتبار ضمن إجراءات الأمن المتبعة، فسريعًا سوف تكتشف المنظمة أن جهودها لتأمين معلوماتها قد ذهبت أدراج الرياح. فعلى شبكة إنترنت بالذات حيث الاتصالات سريعة ومريحة يكفي وجود ثغرة أمنية واحدة في النظام لتهديده، إذ إن هذه الثغرة من الممكن اكتشافها واستغلالها بسهولة. وقد قامت الكثير من المنظمات بحماية شبكاتها باستخدام أسلوب **العزل** وليس أسلوب الأمن، أي بعزل الشبكة تمامًا عن إنترنت وغيرها من الشبكات، ومن ثم فإن المسئولين عن هذه الجهات لا يولون اهتمامًا كبيرًا لقضايا أمن الشبكات، ولكن عندما يمكن الوصول إلى هذه النظم عبر إنترنت، بطريقة أو بأخرى كما سنبين، فمن المحتمل جدًا أن تقع هذه الشبكات بالذات ضحية الاختراق نتيجة اطمئنانها للعزل الذي من المؤكد أن ينعكس على إجراءاتهم الأمنية

وعلى درجة الحذر لديهم، وكثيرًا ما نكتشف أن الشبكة الداخلية للمنظمة قد تم توصيلها (دون أي حماية) بشبكة إنترنت بواسطة وصلة تستخدم (**بروتوكول إنترنت للاتصال المتتالي Serial Link Internet Protocol**) أو (**SLIP**) على سبيل المثال ، وقد يتم هذا الاتصال عن طريق أحد الأقسام غير المتعاونة داخل المنظمة ودون علم مسئولي الشبكة.

من أجل استبعاد فرص وصول أشخاص غير مختصين إلى الشبكات الداخلية تستخدم كثير من المواقع (**نظم بوابات Gateway Systems**) حيث يكون النظام الخارجي (أي الذي يراه مشتركو إنترنت من الخارج) معزولاً عن شبكة الشركة الداخلية، ويتم إرسال واستقبال البريد الإلكتروني وأخبار (**يوزنت Usenet**) بواسطة النظام الخارجي، وبصفة دورية يتم وصل النظام الخارجي بالشبكة الداخلية عن طريق نظام آخر وسيط وباستخدام خط محلي، وبذلك يمكن نقل الرسائل والأخبار المرسلة من الشبكة الداخلية إلى هذا النظام الوسيط (البوابة) ومن ثم إلى النظام الخارجي. وبالعكس يمكن نقل الرسائل والأخبار المستقبلة من النظام الخارجي إلى الشبكة الداخلية عن طريق هذه البوابة.

هذه البوابة المزدوجة تبدو من الناحية الأمنية آمنة تمامًا، ولكن من ناحية ملاءمتها للمستخدم فربما هي ليست كذلك، وبينما هي تسمح للأخبار والبريد بالمرور في كلا الاتجاهين فإن هذا لا يعتبر كافيًا بالنسبة للمستفيدين الذين يحتاجون للوصول إلى بعض خدمات الشبكة التي تحتاج اتصالاً مباشرًا أو تفاعليًا (Interactive)، وكثيرة هي هذه الخدمات ومطلوبة باستمرار كما أوضحنا من قبل.

الأمر الذي يجب ألا يغفله مسئولو أمن المعلومات هو أن دعم ومساندة الإدارة العليا يظل دائمًا هو العامل الأساسي والحاسم لنجاح سياسة تأمين الاتصالات مع شبكة إنترنت.

٧- وسائل الحماية في شبكة إنترنت

٧-١- المشـكلة

من المعروف أن البريد الإلكتروني يعاني من بعض الأخطـار مثـل: خطر الاستقبال غير المرغوب فيه وخطر التنصت ، ومن أجل ذلك يتم اتخاذ الكثير من الاحتياطات مثل: استخدام "**البريد الإلكتروني المؤمَّن**" **(PEM)** أو **(Privacy Enhanced Electronic Mail)** ، وبرغـم أن تـأمين البـريد الإلكتروني يشكل تحديًا حقيقيًا لمستخدمي شبكة إنترنت فإن استخدام البـريد الإلكتروني في الاتصالات الحساسة هو أمر قليل الحدوث. ولكن الأمر الـذي يبدو أكثر خطورة هو التهديد بأن مقتحمًا ما قد يخترق، من خـلال شـبكة إنترنت، نظامًا متصلاً بهذه الشبكة. ويكتسب هذا التهديد أهميته من أمريـن: بينما لا تحتوي الرسالة الإلكترونية إلا على كمية محدودة مـن البيانـات لا تزيد عادة عن بضع مئات أو آلاف من الحروف، فإننا نجد النظم الأخـرى المرتبطة بالشبكة تحتوي على ملايين بل مليارات الحروف أو أكثر من ذلك، الأمر الثاني هو أن المستفيد يدرك جيدًا احتمالات التعرض للاختراق عندمـا يقرر أن يرسل معلومات حساسة في رسالته ويضع هذه الاحتمـالات فـي اعتباره، ولكن مستخدمي النظم المرتبطة بشبكة محلية (LAN) على سـبيل المثال ربما لا يدرون أن الحاسب الكبير الذي يسـتضيف شـبكتهم مرتبـط بشبكة أخرى واسعة النطاق (إنترنت مثلاً) ولذلك فهؤلاء المستخدمون قـد لا يكونون على وعي بالتهديد القائم لكل بياناتهم المخزنة. ولذلك فـإن حمايـة الموارد الأخرى لتلك الشبكات المرتبطة بإنترنت قد اكتسبت أهمية فائقة.

أبسط وسائل الحماية للموارد الحساسة هو عدم ربطها بأي نظام يمكن الوصول إليه من خارج المنظمة، أو بعبارة أدق من خارج "الحدود الآمنـة للمنظمة"، وهذا العزل المادي فعال للغاية في مواجهـة أخطـار الاخـتراق الخارجي. ولكن العديد من المستفيدين يحتاجون، وأكـثر منـهم يريـدون، الوصول إلى خارج هذه الحدود (لاستخدام إنترنت مثلاً). وهنا ربما يقوم أحد

المستفيدين بشراء جهاز مودم رخيص الثمن ويقوم بتركيبه في حاسبه الشخصي الموجود في مكتبه والمرتبط بشبكة المنظمة المحلية، ثم يقوم المستفيد بالاتصال بالخارج عن طريق الهاتف الموجود بمكتبه. هذه الممارسة ربما تكون في غاية الخطورة لأن مسئولي أمن المعلومات لا يعرفون بوجود هذا المودم وبالتالي فهم لا يستطيعون مراقبته أو نصح المستفيد عن كيفية تقليل درجة التعرض لخطر الاختراق، وهم بالطبع لن يقوموا ببناء دفاعات لحماية باقي موارد المنظمة المتصلة بهذا المستفيد الشارد.

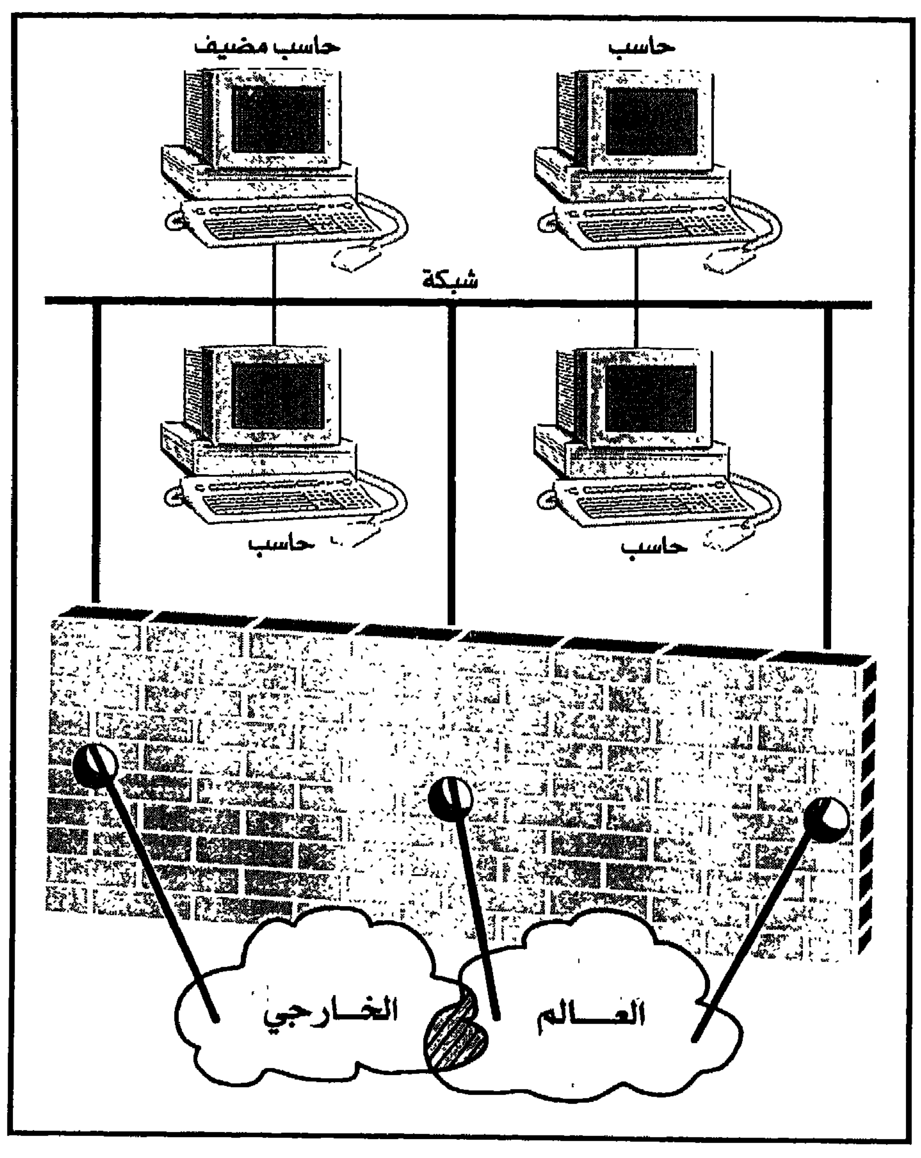
٧-٢- "جدران الحماية" (Firewalls)

هذه المنظمة إذن في حاجة إلى **مصفاة** (فلتر) لا تسمح بالمرور إلا للاتصالات المرغوب فيها فقط وتمنع ما عداها. وفي الوقت نفسه يجب ألا تعوق هذه المصفاة عمليات المستفيد وألا تحرمه من الأنشطة التي يرغب في القيام بها حتى يقتنع هذا المستفيد بعدم الحاجة إلى شراء المودم الخاص به الأمر الذي لو تم قد يفشل مهمة هذه المصفاة تمامًا.

هذه المصفاة المطلوبة تشبه كثيرًا قلاع العصور الوسطى، تلك القلاع التي كانت لها أسوار عالية وقوية تتخللها فتحات ضيقة يستطيع الرماة من خلالها إطلاق أسهمهم على الأعداء. وكانت هذه الفتحات من الضيق بحيث يكاد يكون من المستحيل استخدامها من جانب العدو في إطلاق أسهمه من الخارج إلى الداخل.

هذا النوع من الدفاع يُسمي (**جدار الحماية Firewall**). فجدار الحماية في ذلك الزمان كان حائطًا من الحجارة تتخلله فتحات صغيرة بهدف التحكم بدقة فيما يمر من خلال هذه الفتحات.

ويبين الشكل (١٥-١) جدار الحماية الذي يتولى حماية شبكة محلية من المؤثرات الخارجية.



شكل رقم (١٥-١) جدار الحماية Firewall

٧-٣- ما هو جدار الحماية؟

جدار الحماية هو أداة تصفي (أو تحجز) مرور البيانات بين الشبكة الداخلية المحمية والشبكة الخارجية التي نخشى منها، والهدف منه هو حجز كل ما هو غير مرغوب فيه خارج البيئة المحمية. ولابد أن يطبق جدار الحماية المستخدم سياسة أمنية معينة، هذه السياسة قد تكون مثلاً منع أي دخول من الخارج مع السماح بالمرور من الداخل إلى الخارج. أو قد تسمح هذه السياسة بالدخول من أماكن معينة فقط أو من جانب مستفيدين معينين أو تسمح بالدخول لأنشطة معينة فقط دون باقي الأنشطة. ويعتبر وضع السياسة الأمنية السليمة التي تلبي احتياجات المنظمة هو أحد التحديات الحقيقية التي تواجه المنظمة عندما تقرر حماية شبكتها عن طريق جدار الحماية.

ينقسم مستخدمو جدران الحماية حول التصرف التلقائي (Default) لجدار الحماية، وهناك اتجاهان سائدان هما:

١) الأصل في الأشياء الإباحة أي أن كل ما لم ينص على منعه فهو مباح.

٢) الأصل هو المنع أي أن كل ما لم ينص على إباحته فهو ممنوع.

أما المستفيدون بصفة عامة فهم يفضلون السياسة الأولى (الإباحة)، بينما يفضل خبراء الأمن الاتجاه الآخر بشدة وحماس معتمدين في ذلك على خبرتهم الطويلة . وعلى كل منظمة تنوي تركيب جدار الحماية أن تختار بين إحدى هاتين الطريقتين.

٧-٤- خصائص جدار الحماية

جدار الحماية هو نوع خاص من البرامج الرقابية (Monitors) ويحمل نفس خصائصها أي أنه يجب أن يكون:

١) مستيقظًا دائمًا.
٢) مؤمَّنًا هو نفسه ضد الاختراق.
٣) صغيرًا وبسيطًا بما يسمح بالفحص الدقيق.

عن طريق اختيار موقع جدار الحماية بعناية داخل الشبكة نستطيع أن نطمئن إلى أن أي اتصال بالشبكة لابد أن يمر من خلال هذا الحائط، ويتحقق ذلك باستيفاء المبدأ الأول وهو أن يبقى هذا البرنامج مستيقظًا دائمًا.

وعادة يكون جدار الحماية معزولاً بشكل جيد مما يجعله محصنًا بدرجة عالية ضد عمليات التعديل غير المشروعة، ولتحقيق ذلك كثيرًا ما نرى جدار الحماية مركبًا على جهاز حاسب مستقل متصل مباشرة من إحدى جهتيه بالشبكات الداخلية للمنظمة بينما يكون من الجهة الأخرى متصلاً بالعالم الخارجي، أي أنه يكون همزة الوصل بين الداخل والخارج. هذا "العزل" هو الذي يحقق المبدأ الثاني وهو أن يكون مؤمَّنًا ضد الاختراق.

ويوصي مصممو جدران الحماية بشدة بالاحتفاظ بوظيفة جدار الحماية بسيطة وغير معقدة (المبدأ الثالث).

٨- جدران الحماية ما لها وما عليها

لا يمكن الادعاء بأن جدران الحماية تمثل حلاً نهائيًا لجميع مشكلات أمن الحاسبات، إذ إن جدار الحماية لا يحمي سوى الحدود الخارجية فقط (السور الخارجي للقلعة) ضد المهاجمين من الخارج الذين يحاولون مثلاً تنفيذ برنامج ما أو الوصول إلى بعض البيانات المخزنة على وسائط التخزين الخاصة بالمنظمة، ولكن يجب بصفة عامة أن نضع النقاط التالية في اعتبارنا:

١) لا تستطيع جدران الحماية أن تحمي بيئة معينة إلا إذا تحكمت **بالكامل** في المحيط الخارجي، بمعنى ألا يكون هناك أي اتصال يمكن

أن يمر من خلال هذا المحيط الخارجي دون المرور بجدار الحماية. أما إذا كان هناك ولو شخص واحد داخل المنظمة يتصل بأي عنوان خارجي (عن طريق مودم مثلاً) فإن الشبكة الداخلية بأكملها تكون معرضة للاختراق من خلال هذا المودم.

٢) جدران الحماية لا تحمي البيانات في رحلتها خارج الأسوار، فالبيانات التي تمر بنجاح من خلال جدار الحماية تكون بعد ذلك معرضة للأخطار كغيرها من البيانات.

٣) جدران الحماية هو **الجزء المرئي** من المنظمة بالنسبة للعالم الخارجي وهو أكثر الأهداف جاذبية للهجوم، ولذلك فاللجوء إلى استخدام عدة طبقات (دفاعات) للحماية أو ما نطلق عليه (**الدفاع في العمق**) يكون أفضل من الاعتماد على قوة حائط وحيد.

٤) برغم أن جدران الحماية مصممة لمقاومة محاولات الاختراق فإن قدرتها على المقاومة ليست بغير حدود، ولذلك يتعمد مصممو هذه النظم الإبقاء على هذه الحوائط صغيرة وبسيطة ما أمكن لضمان أنه حتى في حالة نجاح المهاجم في اقتحامها فلن يجد فيها أي أدوات مساعدة (كمترجمات البرامج مثلاً) تساعده على مواصلة الاختراق والذهاب أبعد من هذا الحد.

٥) يجب أن يتم تصميم جدران الحماية بحيث تلائم بيئة العمل، ويجب مراجعة هذا التصميم وتحديثه عند كل تغيير في البيئة الداخلية أو الخارجية، كما يجب الالتزام بمراجعة كل التقارير التي يخرجها جدار الحماية عن نشاطه لاكتشاف أي محاولات اختراق والتنبه لها وربما تعديل التصميم تبعًا لذلك.

٦) لا تقدم جدران الحماية الشيء الكثير في مجال مراقبة المحتويات الفعلية للبيانات التي يتم تمريرها إلى الداخل، ويعني ذلك أن المعلومات غير الصحيحة أو البرامج الضارة يجب مراقبتها داخل الأسوار بوسائل أخرى.

٩- شبكة "إنترنت" في المملكة العربية السعودية

٩-١- من الذي يملك شبكة "إنترنت"؟

يندهش كل من يقدم على الانضمام إلى شبكة إنترنت عندما يكتشف عدم وجود سلطة مركزية للتحكم في الشبكة أو لتنظيم استخدامها. وفي الواقع فالسلطة المركزية الوحيدة هي **"مركز معلومات الشبكة" (NIC)** أو **(Network Information Center)**، وهو المركز الذي يشرف (بقوة العرف وليس بقوة القانون) على توزيع العناوين وأسماء **"النطاقات" (Domains)** من خلال الوحدة المكلفة بتقديم **"خدمة أسماء النطاقات" (DNS)** أو **(Domain Names Service)** لمستخدمي الشبكة. وفيما عدا هذا التدخل المحدود فلا توجد أي جهة رقابية على الشبكة، وحتى مواصفات إنترنت القياسية التي قامت بإعدادها لجنة تسمى **"اللجنة الهندسية للشبكة" (IETF)** أو **(Internet Engineering Task Force)** لا يمكن فرض استخدامها أو الالتزام بها، ولكن يلتزم بها مستخدمو الشبكة من تلقاء أنفسهم، فقط لتحقيق مصالحهم المشتركة.

٩-٢- تنظيم الاستخدام في المملكة

أما في المملكة العربية السعودية فقد أسندت مسئولية تنظيم استخدام شبكة إنترنت والإشراف على تقديم الخدمة إلى "مدينة الملك عبد العزيز

للعلوم والتقنية" وذلك بموجب مرسوم ملكي، فقامت المدينة بإعداد القواعد والأسس التي يتم بناء عليها تقديم الخدمة بواسطة مقدمي الخدمة من القطاع الخاص، وقد تم فتح الباب لتتقدم الشركات الراغبة في تقديم الخدمة. وبالفعل تقدم عدد كبير من هذه الشركات وأعلنت المدينة أنه تم اختيار (٤٦) شركة لتقديم الخدمة على رأسها شركة "الاتصالات السعودية" وهي الشركة التي تكونت في أعقاب خصخصة خدمة الهاتف في المملكة العربية السعودية. ولكن تناقص هذا العدد في الشهور الأولى التي تلت إدخال الخدمة بالمملكة إلى النصف تقريبًا.

١٠- دور الأجهزة السعودية المعنية بأمن المعلومات في ضمان أمن الشبكة

١٠-١- أمن الشبكة

إذا تحدثنا عن **الرقابة (Control)** على شبكة إنترنت بصفة عامة، فمن المؤكد أن الشبكة تعاني من مشكلة **الشيوع** أو عدم الخصوصية، فلا توجد أي سلطة تديرها، وهذا أمر يثير العجب والإعجاب في الوقت نفسه.

وإذا تحدثنا عن **الأمن (Security)** فإن كل جهة مرتبطة بالشبكة تعلم أن عليها أن تتحمل المسئولية الكاملة عن سلامتها وأمنها، فعلى **"طريق المعلومات السريع" (Information Super Highway)**، كما يحلو للكثيرين تسمية الشبكة، لا توجد كمائن للمرور أو الأمن الشامل لفرض الأمن والنظام في هذا الفضاء الواسع.

١٠-٢- دور الأجهزة السعودية

وفي الشق الرقابي والأمني تتولى مدينة الملك عبد العزيز للعلوم والتقنية وضع ضوابط الاستخدام، كما تقوم بوضع "**جدران الحماية**" (**Firewalls**) والأجهزة "**المفوضة**" أو "**الوسيط**" (**Proxy**) لوضع حد أدنى من الرقابة، وقد تحدثنا في هذا الفصل باختصار عن هذه الأنواع من أدوات الرقابة على الشبكة وحفظ الأمن فيها.

ولكن حتى إعداد هذا الكتاب للنشر لم تكن كافة الإجراءات قد انتهت بشكل كامل بعد، كما إن استخدام الشبكة، والذي لم يبدأ إلا في منتصف شهر رمضان ١٤١٩ هـ أي في شهر يناير ١٩٩٩م لم يصل إلى درجة كافية من الاستقرار بعد.

١٠-٣- المخاطر الأمنية على مستوى المملكة العربية السعودية

تحدثنا في هذا الفصل من قبل عن الهموم التي يعاني منها العالم والهموم التي تنفرد بها الدول العربية عن غيرها من الدول، وهذه كلها هموم تدور في الخاطر السعودي وهو ما زال في أول مشوار الإنترنت، ولكن هناك هموم إضافية تنفرد بها المملكة العربية السعودية فيما يخص الشبكة، يأتي على رأسها همان أساسيان هما: عدم خبرة مقدمي الخدمة، والبنية التحتية لشبكات الهاتف، وسنتعرض فيما يلي لهذه الهموم ولكيفية معالجتها:

١٠-٣-١- عدم خبرة مقدمي الخدمة

الهم الأول المتعلق بعدم خبرة مقدمي الخدمة يؤدي إلى حدوث مخاطر أمنية جسيمة تتمثل في عدم التحكم الجيد في أمن البيانات واتخاذ الإجراءات

الأمنية المناسبة في الحفاظ على أمن المعلومات المتداولة عن طريقهم، كما تتمثل في الخشية من ضياع الرسائل أو تأخر وصولها إما لقلة الخطوط الممنوحة لهم أو حالات انقطاع الخدمة التي لوحظت كثيرًا في الشهور الأولى لدخول خدمة إنترنت إلى المملكة ، وتتمثل أيضًا في صعوبة الاتصال بمقدم الخدمة إذا كانت اشتراكات العملاء لديه أكثر من طاقته في الاستيعاب وطاقة الخطوط الممنوحة له.

لم يمكن بعد تقييم الدور الذي تقوم به مدينة الملك عبد العزيز للعلوم والتقنية كجهة مركزية يتم من خلالها اتصال كافة مقدمي الخدمة بالشبكة العالمية، ولو أن الملاحظ أن المدينة ركزت اهتمامها في جدران الحماية وحجب المعلومات عن طريق رصد وتحديث القوائم السوداء للمواقع التي لا ترقى فوق مستوى الشبهات، كما أنها أولت اهتمامًا كبيرًا لتنظيم تسعيرة الاشتراك التي تلزم بها مقدمي الخدمة. ولكننا كنا ننتظر من مدينة الملك عبد العزيز للعلوم والتقنية ، بعد اختيارها للإشراف على ملف الإنترنت بالمملكة، قيامها بدور أكبر وأخطر وهو التوعية ونشر ثقافة الإنترنت بالمملكة ولكن يبدو أنها أفلتت من بين يديها هذه الفرصة الذهبية، على الأقل في الوقت الحاضر.

١٠-٣-٢- البنية التحتية لشبكات الهاتف

الهم الثاني من هموم الشبكة في المملكة ليس مشكلة هينة وإنما هي مشكلة حقيقية، ونعني بها البنية التحتية للاتصالات أي شبكات الهاتف التي لا تسمح بسرعات كبيرة لتبادل البيانات. ويحد ذلك كثيرًا من أحجام البيانات المتبادلة، كما يحد من إمكانية استخدام بعض الخدمات مثل (الائتمار عن بعد Teleconferencing) حيث يستطيع عدة أشخاص في بلاد مختلفة أن يعقدوا مؤتمرًا بالصوت والصورة عبر الشبكة مثلما نرى على شاشة (CNN) أو (MBC) أو غيرها من الشبكات الإخبارية.

يجرى الآن مشروع لتوسعة شبكة الهاتف في المملكة، والذي يهدف إلى توسعة وتحسين شبكات الهاتف وإدخال الخطوط السريعة مثل "كابلات" الألياف البصرية لربط مدن المملكة لتكون هي العامود الفقري للشبكة، ومعروف أن هذه الأنواع من "الكابلات" تمتاز بعدة خصائص منها سرعة نقل المعلومات وزيادة السعة (Bandwidth) مما يسمح بنقل عدد أكبر من المكالمات آنيًا عبر "الكابل"، كما أنها تمتاز بمناعتها الكبيرة ضد الشوشرة أو التشويش (Noise). وسيحتاج الأمر إلى تغيير بعض المقاسم القديمة التي تشكل في الوقت الحالي عنق زجاجة، والتي لا يمكن حتى الآن تقديم خدمة الإنترنت من خلالها مما يحرم قطاعات كبيرة في المملكة من هذه الخدمة في الوقت الحالي ليس فقط في المدن الصغيرة ولكن في العاصمة الرياض وجدة والدمام كذلك.

ولكن ما سوف ينتقل بالمملكة فعلاً إلى عصر المعلومات وينشئ بها شبكة معلومات حقيقية بمعنى الكلمة هو إدخال التقنيات الرقمية أو ما نطلق عليه "الشبكة الرقمية للخدمات المتكاملة" (ISDN) التي يمكن من خلالها تبادل المعلومات الرقمية، وليس التناظرية كما هو عليه الحال الآن، ونستطيع بذلك أن ننقل خدمات الصوت والصورة والفيديو إلى جانب بيانات الحاسب معًا في تكامل.



المراجع

1- Abrams, Marshall D. & Podell, Harold J.: "Malicious Software". Book chapter of "Information Security an integrated collection of essays" Essay 4 p.p. 111 Edited by Abrams, Marshall D. Jajodia, Sushil & Podell, Harold J. IEEE Computer Society Press California U.S.A. 1998.

2- Bates, Regis J.: "Disaster recovery for LANs: a planning and action guide" McGraw-Hill 1994.

3- Bidzos, D. James: "Public Key Cryptography" Book chapter (Ch. 13 in "Computer Security Reference Book" edited by Jackson, K.M. & Hruska, J.) Butterworth - Heinemann 1992.

4- Bowers, Dan M.: "Access Control & Personal Identification Systems" Butterworths 1988.

5- Bulgawicz Susan L. & Nolan, Charles E.: "Disaster Prevention & Recovery: a planned approach" ARMA International 1988.

6- Caelli, William: "Information Security for managers" 1989.

7- Carr, Indira Mahalingam & Williams, Katherine S.: "Bytes in Computer Law" Book Chapter one in "Computers and law" Edited by Carr, Indira & Williams, Katherine. Intellect Oxford - London 1994.

8- Clark, D.: "The Clipper Chip's Flaw may force change in Encryption Design for Computers" The Wall Street Journal June 3, 1994.

9- Cohen, Frederic: "Computer Viruses" Book chapter (Ch. 44 in "Computer Security Reference Book" edited by Jackson, K.M. & Hruska, J.) Butterworth - Heinemann 1992.

10- Collier, P. A. & Spaul B. J.: "A Forensic Methodology for countering Computer Crime" Book Chapter in "Computers and law" Edited by Carr, Indira & Williams, Katherine. Intellect Oxford - London 1994.

11- Daler, Torgeir Gulbrandsen, Roar Melgard, Birger Sjolstad, Torbjorn: "Security of Information & data" John Wiley (Ellis Horwood) Chichester 1989.

12- Denning, D.: "The Clipper Encryption System", American Scientist, July-August 1993 pp. 319-323.

13- Diffle, W. and Hellman, M.: "New directions in cryptography", IEEE Transactions on Information Theory, November 1976, pp. 644-654.

14- Durr, Michael: "Networking IBM PCs. a practical guide", 1987.

15- Elbra, R.A.: "Computer Security Handbook", 1992.

16- Fites, Philip Johnston, Peter Kratz, Martin: "The Computer Virus Crisis" 2nd edition, 1992.

17- Helman, M.: "A Cryptoanalytic Time-Memory Trade off" IEEE Transaction Information Theory, v IT-26 n.4 July 1980 pp.401-406.

18- Highland, Harold Joseph: "Computer Virus Handbook" Elsevier Advanced Technology Oxford U.K. 1990.

19- Hoeren, Thomas: "Electronic Data Interchange: the Perspectives of Private International Law and Data Protection" Book Chapter in "Computers and law" Edited by Carr, Indira & Williams, Katherine. Intellect Oxford - London 1994.

20- Hutt, Arthur E. et al: "Computer Security Handbook" 3rd edition, John Wiley & Sons. 1995.

21- Jackson, K.M.: Book chapter (in "Computer Security Reference Book" edited by Jackson, K.M. & Hruska, J.) Butterworth - Heinemann 1992, pp. 652.

22- Jackson, K.M.: "Computer Security Reference Book" edited by Jackson, K.M. & Hruska, J.) Butterworth - Heinemann, 1992.

23- Knight, Peter: "Network Management" British Standards Institution 1992.

24- Lejk, Mark and Deeks, David: "An introduction to Systems Analysis Techniques" Prentice Hall, 1998.

25- Louw, Eric & Duffy Neil: "Managing Computer Viruses" Oxford University Press U.K. 1992.

26- Martin, R. Smith: "Commonsense Computer Security: your practical guide to preventing accidental and deliberate data loss", 1989.

27- O'Shea, G.: "Security in Computer Operating Systems" NCC Blackwell 1991.

28- Official Journal: "Revised Draft Directive" No. L123 May, 8 1992.

29- Palmer-Stevens, David: "The Cabletron Systems Guide to Local Area Networking", Cabletron Systems, 1992 .

30- Park, Joseph S.: "AS/400 Security in a Client / Server Environment" John Wiley 1995.

31- Pfleeger, Charles P.: "Security in Computers" 2nd edition, Prentice Hall, 1997.

32- Rankin, Bob: "Dr. Bob's Painless guide to the INTERNET", William Pollock Publisher, 1996.

33- Shimmin, Bradley: "Effective E-Mail" Academic Press Prfessional, 1997.

34- Smid, M., and D. Branstad: "The Data Encryption Standard: Past Present and Future" Proceedings of IEEE v76 n5, May 1988, pp. 550-559.

35- Stoll, Clifford: "The Cuckoo's Egg", Bantam Doubleday Dell Publishing Group, 1989.

36- Wong, Ken: "Managing Information Security: a non-technical management guide" 1990.

37- Wood, Michael B.: "Guidelines for physical computer security", 1986.

38- Write, B.: "The verdict on plain text signatures: They're legal", Communications of the ACM, October 1994, p. 122.

٣٩-داود، حسن طاهر: "جرائم نظم المعلومات"، أكاديمية نايف للعلوم الأمنية، الرياض، ٢٠٠٠م.

٤٠-"معجم مصطلحات الحاسبات الإلكترونية"، مركز الأهرام للترجمة والنشر، القاهرة، ١٩٨٧م.



ملحق رقم ١

خطة طوارئ مقترحة

لمركز الحاسب الآلي

بمعهد الإدارة العامة



هذه الخطة

هذه الخطة المقترحة تم إعدادها في عام ١٤١٧هـ (١٩٩٦م) بواسطة عدد من المتدربين ضمن برنامج "إدارة مراكز الحاسب الآلي" الذي يقدمه معهد الإدارة العامة بالرياض. وهؤلاء المتدربون كانوا من مديري مراكز الحاسب الآلي بالمملكة العربية السعودية وبعض الدول العربية، وكان هذا النشاط ضمن مادة "أمن وسرية المعلومات" التي قمت بتدريسها ضمن هذا البرنامج. ولم يكن لي من جهد في إعداد هذه الخطة سوى جهد الإشراف والتوجيه، ولكنني قمت عند إعداد هذا الملحق بإدخال كافة التعديلات الضرورية على ما قاموا به بهدف اكتمال الفائدة. لذلك أود أن أنوه بجهد هؤلاء الأصدقاء وأوجه لهم الشكر الجزيل، وهم:

محمد عبدالله الألمعي	يحيى عبدالعزيز الحشر
محمد عبدالعزيز المفلح	محمد عبدالرحمن المشاري

قائمة المحتويات

(١) المقدمة

أ ـ تمهيد

يهدف هذا المشروع إلى إعداد خطة الطوارئ الخاصة بمركز الحاسب الآلي بمعهد الإدارة العامة، وقد تم إعداد هذه الخطة (من أجل استعادة النشاط بمركز الحاسب الآلي في أسرع وقت ممكن وبأقل تكلفة) وللتقليل من حجم المخاطر والأضرار التي تنتج من وقوع الكارثة، وذلك للأهمية البالغة لنظم الحاسب الآلي في إنجاز مهام معهد الإدارة العامة وأدائه لرسالته النبيلة بالمساهمة الفعالة في تحقيق (تنمية إدارية أفضل) لمجتمعنا وبلادنا الحبيبة... مما يستوجب وجود خطة طوارئ فعالة استناداً إلى توجيهات الإدارة العليا للمعهد بضرورة ضمان استمرارية عمل المعهد ومزاولته لنشاطه وأدائه لدوره الهام في أقصر وقت ممكن عند حدوث المخاطر لا قدر الله، وأن يكون ذلك بأقل تكاليف ممكنة، وهذا هو ما قام به فريق هذا المشروع الذي تولى إعداد هذه الخطة بالتعاون والتنسيق مع المسؤولين والمختصين بالإدارات المعنية بمعهد الإدارة العامة وتحت إشراف مهندس/ حسن طاهر داود أستاذ مادة أمن وسرية المعلومات بمعهد الإدارة العامة بالرياض.

والله من وراء القصد.

فريق المشروع

ب ـ التزام الإدارة العليا

بسم الله الرحمن الرحيم

المملكة العربية السعودية
معهد الإدارة العامة

قرار إداري رقم وتاريخ / /١٤١٧هـ

إن المدير العام لمعهد الإدارة العامة بالرياض وبناء على ما له من صلاحيات، ولأهمية وجود خطة طوارئ لنظام الحاسب الآلي بمركز الحاسب الآلي بالمعهد، وبناء على خطة الطوارئ المعروضة عليه من فريق العمل المكون من بعض الدارسين بالدورة السادسة لمديري مراكز الحاسب الآلي المنعقدة بالمعهد، وبعد الاطلاع عليها، يقرر ما يلي:

(١) الموافقة على خطة الطوارئ لمركز الحاسب الآلي بالمعهد واعتمادها. المرفق رقم (١).
(٢) على مدير عام الشئون المالية والإدارية بالمعهد الارتباط بتكاليف تنفيذها ومقدارها (٧٥٠,٠٠٠) ريال.
(٣) على نائبنا لشئون البحوث والمعلومات إنفاذه وإبلاغه لمن يلزم للتمشي بموجبه.

وبه حرر.

مدير معهد الإدارة العامة

ج ـ الجهات المشاركة في تنفيذ الخطة:

- نائب مدير عام المعهد لشئون البحوث والمعلومات.
- مركز الحاسب الآلي.
- إدارة العمليات بمركز الحاسب الآلي.
- إدارة التطبيقات بمركز الحاسب الآلي.
- إدارة خدمات المستفيدين بمركز الحاسب الآلي.
- إدارة القبول والتسجيل.
- إدارة الصيانة والتشغيل.
- إدارة الشئون المالية.
- إدارة العلاقات العامة.

(٢) أهداف خطة الطوارئ

أ - تعريف الخطة:

هي خطة مكتوبة ومعتمدة ومعلنة ومعدة للتنفيذ ويتم اختبارها باستمرار، وهي تحدد كافة الإجراءات الواجب اتخاذها لتحسين درجة مقاومة المؤسسة للأخطار وتقليل الخسائر الناتجة عن الكارثة عند حدوثها إلى الحد الأدنى.

ب - فوائد خطة الطوارئ وأهدافها:

إن خطة مواجهة الطوارئ هي نهاية المطاف في نشاط مواجهة الكوارث في أي منظمة، ولذلك فإن هدفها (هو استعادة المنظمة لنشاطها في أقصر وقت ممكن وبأقل تكلفة ممكنة) وتحقيق هذين الهدفين المتعارضين يتطلب الكثير من الدراسة والدقة في إعداد خطة ألطوارئ وبنائها على أسس صحيحة، حيث إن الاستعادة الفورية للنشاط الحرج (لمعهد الإدارة العامة) يتطلب تكلفة مرتفعة ولذلك لابد من الحساب الدقيق لهذين العاملين (سرعة استعادة النشاط والتكلفة المطلوبة) والعلاقة بينهما حتى يمكن التوصل إلى أفضل حل يوازن بينهما.

ومن أجل تحقيق ذلك نستطيع أن نوجز أهداف خطة الطوارئ لنظام الحاسب الآلي بالمعهد فيما يلي:

(١) ضمان استمرارية العمل الرئيسي لمعهد الإدارة.

(٢) التقليل من الخسائر التي قد تنجم عن الأخطار لمركز الحاسب الآلي بشكل عام والنظام الحرج بشكل خاص.

(٣) المحافظة على سرية البيانات.

(٤) المحافظة على سلامة وتكامل البيانات.

(٥) المحافظة على مستوى الثقة وسمعة المعهد لدى الجهات الأخرى المعنية وغيرها.

(٦) سرعة استعادة النشاط.

ج - النشاط الرئيسي للمعهد

١) معهد الإدارة العامة بالرياض وأهدافه وأولوياته

معهد الإدارة العامة تابعة لوزارة الخدمة المدنية أُنشأ بموجب المرسوم الملكي رقم ٩٣ وتاريخ ١٣٨٠/١٠/٢٤هـ الموافق ١٠ إبريل ١٩٦١م، ومهمته المساهمة بفاعلية تحقق تنمية إدارية أفضل، ويقوم على رسم سياسة المعهد مجلس إدارة برئاسة معالي وزير الخدمة المدنية، ويعتبر هذا المجلس السلطة المهيمنة على شئون المعهد وهو الذي يحدد السياسة العامة للمعهد ويبت في أموره الإدارية والمالية.

٢) المهام المنوطة بالمعهد:

حددت المادة الثالثة من نظام المعهد هذه المهام على النحو الآتي:

- وضع وتنفيذ برامج تعليمية وتدريبية للمستويات الوظيفية المختلفة.
- إجراء البحوث والدورات الإدارية العلمية وتوجيهها والإشراف عليها والتعاون مع المسؤولين في الوزارات والمصالح الحكومية وفروعها عندما يكون البحث ميدانيًا بأي منها.
- جمع وتبويب وتصنيف الوثائق الإدارية بالمملكة.
- القيام بعقد مؤتمرات التنمية الإدارية للمستويات العليا من موظفي الدولة.
- الدعوة إلى مؤتمرات عربية وإقليمية ودولية بالمملكة في شئون الإدارة العامة والاشتراك في مثيلاتها بالخارج.

- نشر البحوث العلمية في شئون الإدارة وتبادلها مع الجهات المعنية بالمملكة وبالدول العربية وغيرها من الدول.
- تشجيع البحوث العلمية في شئون الإدارة، وتقرير المنح الدراسية والمكافآت لهذا الغرض.
- إيفاد بعثات علمية وتدريبية في علوم الإدارة لينتفع بأعضائها في التدريب بالمعهد ورفع الكفاءة الإدارية بين الموظفين.
- قبول دارسين من أبناء الدول العربية.
- يجوز للمعهد أن يستعين بالمساعدات الفنية والمالية التي تقدمها المؤسسات والهيئات الحكومية.

٣) إدارات المعهد

يعمل المعهد على تحقيق أهدافه المرسومة حسب أولويتها من خلال نشاط إداراته المختلفة والتي تقوم بتقديم الخدمات التالية:

- **البرامج التدريبية** (تدريب على رأس العمل) لموظفي الدولة لرفع مهارتهم وزيادة كفاءتهم.
- **البرامج الإعدادية** (قبل الخدمة) حيث يعتبر التدريب الإعدادي مصدراً هامًا من مصادر توفير القوى العاملة لسد احتياجات الدولة المختلفة بموظفين تم تأهيلهم خصيصًا لشغل وظائف معينة.
- **البرامج العليا:** تنظم إدارة البرامج العليا الحلقات العلمية والندوات لفئة الإدارة العليا بالأجهزة الحكومية وغيرها بهدف تعريفهم بآخر التطورات في حقول تخصصهم وتبادل الآراء حول المشكلات الإدارية المعاصرة من واقع الإدارة بالمملكة.

- **البرامج الخاصة** لبعض الجهات الحكومية والأهلية التي لا تتوفر لها برامج ضمن البرامج التدريبية التي يقترحها المعهد بصفة دورية.
- **مركز اللغة الإنجليزية:** حيث يقوم بتنفيذ دورات في مجال تعليم اللغة الإنجليزية للأشخاص المقرر ابتعاثهم للخارج، ولمن تتطلب أعمالهم إجادة اللغة الإنجليزية.
- **الاستشارات:** هي وسيلة ناجحة أخرى يقوم المعهد بتقديمها للأجهزة الحكومية الأهلية حول المشكلات التي تواجههم.
- **الأمانة العامة للجنة العليا للإصلاح الإداري:** وتقوم بإعداد الدراسات التنظيمية والإجرائية اللازمة بالإضافة إلى تنسيق كافة نشاطات اللجنة العليا واللجنة التحضيرية.
- إدارة **البحوث:** وتمثل المساهمة الثالثة للمعهد لدفع عجلة (التنمية الإدارية) حيث تقوم إدارة البحوث بدعم وتشجيع البحث العلمي بشقيه المكتبي والميداني بالإضافة إلى الإشراف على مجلة متخصصة هي مجلة الإدارة العامة.
- **مركز التوثيق:** ويهتم بالوثائق الإدارية والقرارات والأنظمة التي وضعت خلال التطور التاريخي في المملكة، ويحتوي المركز على عدد ضخم من الوثائق الإدارية تمثل مصدراً زاخراً من المعلومات للكتاب والباحثين.
- **النشر:** حيث أنشأ المعهد إدارة للنشر تقوم بطباعة ونشر المذكرات والكتب والبحوث التي تصدر عن المعهد، وأنشأ المعهد مطبعة خاصة لتسهيل عملية طباعة البحوث والدراسات وتوزيعها.

٤) فروع المعهد:

يتولى المعهد تنفيذ المهمات السابقة من خلال مركزه الرئيسي في مدينة الرياض وفرعيه في كل من مدينة جدة (بمنطقة مكة المكرمة) ومدينة الدمام (بالمنطقة الشرقية) إلى جانب فرع خاص للتدريب النسوي في (مدينة الرياض).

د ـ نظم الحاسب الآلي الحرجة والمؤثرة على أداء المعهد:

يوجد في كل منظمة بعض نظم التطبيقات الحرجة أو الحساسة والتي يؤدي توقفها إلى نتائج غير مرغوب فيها، ويعتبر التطبيق حرجًا إذا كان:

(١) يعتمد عليه المعهد في تلبية احتياجاته.
(٢) يتأثر به أداء الموظفين الأساسين بشدة.
(٣) مطلبًا أساسيًا لتنظيم العمل.
(٤) يحافظ على الصورة العامة للمعهد.
(٥) يمنح المعهد القدرة على المنافسة في مجاله.
(٦) يؤثر بشدة على الخدمة المقدمة لموظفي الدولة.
(٧) يؤثر بشدة على الدخل المالي للمعهد.
(٨) يترتب على توقفه آثار قانونية، إما للمعهد أو المستفيدين من خدماته.
(٩) لا يمكن إحلاله بنظام يدوي كامل وفعال يمكن تطبيقه والاستفادة منه بسرعة.
(١٠) يتطلب معالجة أحجام ضخمة من البيانات.
(١١) يتعامل مع البيانات بالأسلوب المباشر (Online) ولا يمكن أن يتم بأسلوب الدفعات (Batch).
(١٢) حرجًا بالنسبة لنظام آخر.
(١٣) يتطلب تكلفة عالية لاستعادة النشاط.

أما النظم غير الحرجة بالنسبة للمعهد فلا تعامل بنفس الاهتمام، ويكون

النظام غير حرج في الأحوال الآتية:

[١] إذا لم ينطبق عليه أي شرط من شروط النظم الحرجة.

[٢] إذا كان ممكنًا الاستغناء عنه لبضعة أسابيع.

[٣] إذا وجد له بديل يدوي (أو غير يدوي) يمكن تطبيقه والاستفادة منه بسرعة.

ولقد اتضح من استعراض نشاطات معهد الإدارة العامة المذكورة سابقًا أن النشاط الرئيسي للمعهد هو (التدريب) الذي يتم تنفيذه على مستويات مختلفة سواء للموظفين على رأس العمل أو عن طريق البرامج الإعدادية للقوى العاملة لتهيئتها للانخراط في خدمة الوطن.

ونتيجة استخدام وسائل التقنية الحديثة في جميع المجالات فإن معهد الإدارة العامة كان ضمن الجهات التدريبية والتعليمية الهامة التي استخدمت نظام الحاسب الآلي في كافة الأمور المتعلقة بالتدريب ومتطلباته، ولذلك فإن نظام الحاسب الآلي الخاص بالتسجيل وجميع النظم والبرامج المرتبطة به والمتفرعة منه هي أنظمة حرجة بالنسبة للمعهد.

هـ - كيفية تحديد النظام الحرج ودرجة أهميته للمعهد:

تم التوصل إلى معرفة النظام الحرج بالمعهد ودرجة أهميته وحساسيته وفقًا للدراسة التالية:

عدد	اسم النظام	سبب الأولوية	هل هو حرج؟ نعم	هل هو حرج؟ لا	درجة الأهمية والحساسية	ملاحظات
١	نظام التسجيل	تتوقف عليه العملية التدريبية بشكل كبير.	✓		%٩٥	لقد تم ترتيب الأولوية بناء على المقابلات مع المسـئولين والمختصين بمعظم إدارات المعهد التي لها علاقة بمشروع خطة الطوارئ لنظم الحاسب الآلي بمعهد الإدارة العامة بالرياض ومنها إدارة خدمات المستفيدين، إدارة العمليات، إدارة التطبيقات بمركز الحاسب الآلي، وإدارة القبول والتسجيل.
٢	نظام جدولة المحاضرات، والقاعات والأساتذة.	يقوم بجدولة القاعات والمحاضرات والأساتذة وتنسيق جميع ذلك.	✓		%٧٥	
٣	نظام بطاقات المهام	مرتبط بـ (٢)	✓		%٧٥	
٤	نظام تقويم التدريب	مرتبط بـ (١)		✓		
٥	نظام الإسكان	مرتبط بـ (١)		✓		
٦	نظام مكافآت المتدربين	مرتبط بـ (١)		✓		
٧	نظام الشئون المالية وتوابعه ومن ضمنها نظام الرواتب	جميع الإجراءات المالية بالمعهد تتم آليًا لهذا النظام وتوابعه.		✓	%٧٠	
٨	نظام المكتبة والتوثيق	إجراءات المكتبة والإعارة آليًا وكذلك الحصول على الوثائق.		✓	%٦٥	

(٣) تحليل المخاطر

أ ـــ منهجية تحليل المخاطر:

تحليل المخاطر في مجال تقنية المعلومات هو التقنية المستخدمة لتقليل درجة تعرض مركز الحاسب أو شبكة المعلومات مثلاً للمخاطر بأنواعها، ويجب أن ينفذ هذا النشاط خلال مرحلة تصميم أي نظام لأن إجراءات الأمن التي يتم تضمينها للنظام منذ البداية تكون أكثر فاعلية من تلك التي تضاف للنظام في مراحل لاحقة.

وتتضمن منهجية تحليل المخاطر:

- تحديد أصول المعهد الممثلة في موارد الحاسب جميعها.
- تقييم الأصول بتحديد أهمية كل أصل من هذه الأصول للمعهد.
- تحديد الأخطار واحتمالاتها وتقرير حد المخاطرة المقبول لدى المعهد.
- اختبار إجراءات التأمين التي تقلل المخاطرة إلى الحد المطلوب.
- مراجعة فاعلية الإجراءات المتخذة والتأكد من نجاحها.

ويجب أن تتم مراجعة فاعلية الإجراءات باستمرار نظرًا لتغير الكثير من العوامل التي بنيت عليها هذه الإجراءات وذلك لأنه بمرور الوقت تتغير قائمة الأصول وقيمة هذه الأصول.

ب ـــ تحديد وتقييم أصول مركز الحاسب

في هذا الجزء من الدراسة نحاول أن نتعرف على أصول مركز الحاسب التي تقوم بخدمة معهد الإدارة العامة بالرياض، وكذلك نقوم بتقييم هذه الأصول وذلك من خلال المعلومات التي تم جمعها من جميع المختصين.

نوع الأصل	التكلفة		الخسارة المتوقعة	ملاحظات
	مباشرة	غير مباشرة		
الأصول البرمجية				
MVS	٢٠,٠٠٠	لا توجد	٢٠,٠٠٠	استئجار شهري
OMEGAMON	٨٠,٠٠٠		٨٠,٠٠٠	استئجار شهري
JES2	٢٠,٠٠٠		٢٠,٠٠٠	استئجار شهري
VTAM	١٧,٠٠٠		١٧,٠٠٠	استئجار شهري
CICS	٣٥,٠٠٠		٣٥,٠٠٠	استئجار شهري
TSO	٢٣,٠٠٠		٢٣,٠٠٠	استئجار شهري
الأصول المادية				
أجهزة الحاسب				
معالج رئيسي CPU	٣٠٠,٠٠٠		٣٠٠,٠٠٠	شراء
أقراص تخزين DASD	١,٥٠٠,٠٠٠		١,٥٠٠,٠٠٠	شراء
جهاز قراءة الأشرطة	١,٠٠٠,٠٠٠		١,٠٠٠,٠٠٠	شراء
وحدات تحكم CONTROL	٥٠٠,٠٠٠		٥٠٠,٠٠٠	شراء
الطرفيات				
شاشات IBM	٧٠,٠٠٠		٧٠,٠٠٠	شراء
أجهزة الإخراج				
طابعات IBM	٥٠٠,٠٠٠		٥٠٠,٠٠٠	شراء

ج ـ تحديد الخسائر المتوقعة:

نظرًا لاعتماد المعهد على النظم الآلية الموجودة لديه اعتمادًا كليًا، فإنه قد تحدث كارثة في حالة فقد أو إفشاء أو تزوير أو تدمير أحد الأنظمة أو البرامج. وقد تم التركيز على الخسائر التي ستصيب النظم الحرجة للمعهد لأهميتها الفائقة.

النظام الحرج	فقد	إفشاء	تدمير	تزوير
برامج التسجيل	٢٠٠,٠٠٠	١٠٠,٠٠٠	٥٠٠,٠٠٠	٢٠٠,٠٠٠
برامج بطاقات المهام	١٥٠,٠٠٠	٥٠,٠٠٠	١٠٠,٠٠٠	٢٠٠,٠٠٠
برامج الجدولة	١٥٠,٠٠٠	١٠٠,٠٠٠	٣٠٠,٠٠٠	٨٠,٠٠٠

من الجدول السابق يتضح لنا أن التكلفة التي يتحملها المعهد نتيجة تعطل النظام الحرج تبلغ (١,٠٠٠,٠٠٠) مليون ريال، وذلك مجموع أكبر خسارة لكل نظام من الأنظمة السابقة:

٥٠٠,٠٠٠ + ٢٠٠,٠٠٠ + ٣٠٠,٠٠٠ = ١,٠٠٠,٠٠٠ ريال

د ـ تحديد الأخطار التي يتعرض لها كل أصل

الأصـــــل	الحريق	السرقة	الإغراق	الصواعق	الزلازل	البراكين	الفيضان	الفقد	التعطل
وحدة المعالجة المركزية CPU	%٣٥	%٥	%٥					%١٠	%١٥
أقراص التخزين DASD	%٣٥	%٥	%٥					%١٠	%٢٠
وحدة قراءة الأشرطة	%٣٥	%٥	%٥					%١٠	%٢٠
أشرطة البيانات	%٥	%٣٠	%٥					%٥	%٣٠
وحدات التحكم	%٣٥	%٥	%٥					%١٠	%٣٠
شاشات IBM	%٢٠	%٢٠	%٢					%١٠	%٥
طابعات IBM	%٢٥	%١٥	%٢					%١٠	%١٠
أجهزة إدخال	%٢٠	%٢٠	%٢					%١٠	%١٠
الأصول البرمجية									
MVS									%١٥
OMEGAMON									%١٥
JES2									%١٥
VTAM									%١٥
CICS									%١٥
TSO									%١٥
نظام التسجيل		%١٠							%٢٠
نظام الجدولة		%١٠							%٢٠
نظام بطاقات المهام		%١٠							%٢٠

هـ ـ درجة التعرض للأخطار:

درجة التعرض للأخطار هي درجة الضعف أو الخلل في نظام معلومات والذي يمكن أن يستغل ليسبب ضرراً للنظام، وكلما زادت درجة التعرض للخطر زاد تأثير الخطر على الأصول عند وقوعه.

ولكي نتمكن من معرفة درجة التعرض للأخطار كان لابد من مقابلة المديرين والموظفين وذلك لمعرفة مكامن الخطر في مركز الحاسب الآلي بالمعهد وكذلك التعرف على الأصول بشكل أكثر دقة وطرق توصيل "الكوابل" الكهربائية والخطوط التليفونية ومن خلال هذه المقابلات تمكنا من تحديد احتمال التعرض للخطر بشكل أكثر دقة ووجدنا ضرورة اتخاذ الإجراءات المناسبة لحماية أصول المعهد. وفيما يلي نتيجة دراسة درجة التعرض لمركز الحاسب:

١ــ **حماية المبنى:** يوجد بالمبنى أجهزة إنذار صوتية تستخدم عند وقوع الكارثة بالإضافة إلى حرس الأمن الليلي.

٢ــ **حماية غرفة الحاسب الآلي:** يوجد أجهزة إنذار بالحريق، وأجهزة إطفاء. كما تستخدم بطاقات دخول ممغنطة لدخول غرفة الحاسب ، ويوجد جهاز لقياس الحرارة والرطوبة وأجهزة تبريد لحفظ مستوى درجة حرارة ثابت.

٣ــ **الوقاية من أضرار الحريق:** يوجد غاز الهالون لإخماد الحريق.

٤ــ **حماية الخدمات الأساسية:**

أ. **مصدر الطاقة الكهربائية:** يوجد مولد كهرباء بالإضافة إلى بطاريات خاصة تقوم بتوليد الكهرباء لفترة محددة.

ب. **النهايات الطرفية والطابعات:** تتم صيانة الأجهزة من قبل الشركة الموردة وهي شركة (AMDHAL)

ج. **الموقع البديل:** لا يوجد موقع بديل.

٥ـ **وسائط المعلومات:** يتم نسخ البيانات بشكل دوري، ووضعها في مكان آمن بعيدًا عن مواقع الخطر.

ومن أهم الأسباب التي تزيد من درجة تعرض نظام الحاسب الآلي بمعهد الإدارة للخطر ما يلي:

١- **عدم فاعلية الإجراءات الأمنية المتخذة:** حيث إنه بإمكان أي فرد سواء من الزوار أو من المتدربين داخل المعهد أو عمال النظافة الدخول إلى المركز بدون بطاقة دخول.

٢- **عدم كفاية تدريب وتوعية الموظفين في مجال الأمن:** وذلك لعدم وجود أي شخص متفرغ كمسئول عن أمن المعلومات، وأيضًا لعدم وجود الوقت الكافي لدى الموظفين، وربما كذلك لعدم إحساس الموظفين بالخطر إلا بعد حدوثه.

٣- **إجراءات استعادة النشاط غير كافية:** وهذا سبب قوي ومؤثر حيث إنه لا توجد إجراءات لاستعادة النشاط نظرًا لعدم وجود خطة طوارئ أصلاً.

٤- **قصور خطة الطوارئ:** سبق الذكر أنه لا توجد خطة طوارئ للمعهد.

٥- **نظام الاتصالات غير موثوق به:** وذلك من خلال بعض الأخطاء في الاتصالات وتعطل الشبكة في بعض الأحيان وتداخل الخطوط.

٦- **إجراءات الإدخال والإخراج غير آمنة:** حيث إنه من الممكن الوصول إلى المخرجات التي يتم طباعتها بسهولة نظرًا لوجود الطابعات في غرفة يمكن للجميع الوصول إليها والاطلاع على المطبوعات.

٧- **عدم فاعلية ضوابط دخول الأفراد لغرفة الحاسب:** حيث إن الأفراد يمكنهم الدخول إلى غرفة الحاسب بسهولة نظرًا لعدم وجود بطاقات يبرزها الفرد عند الدخول.

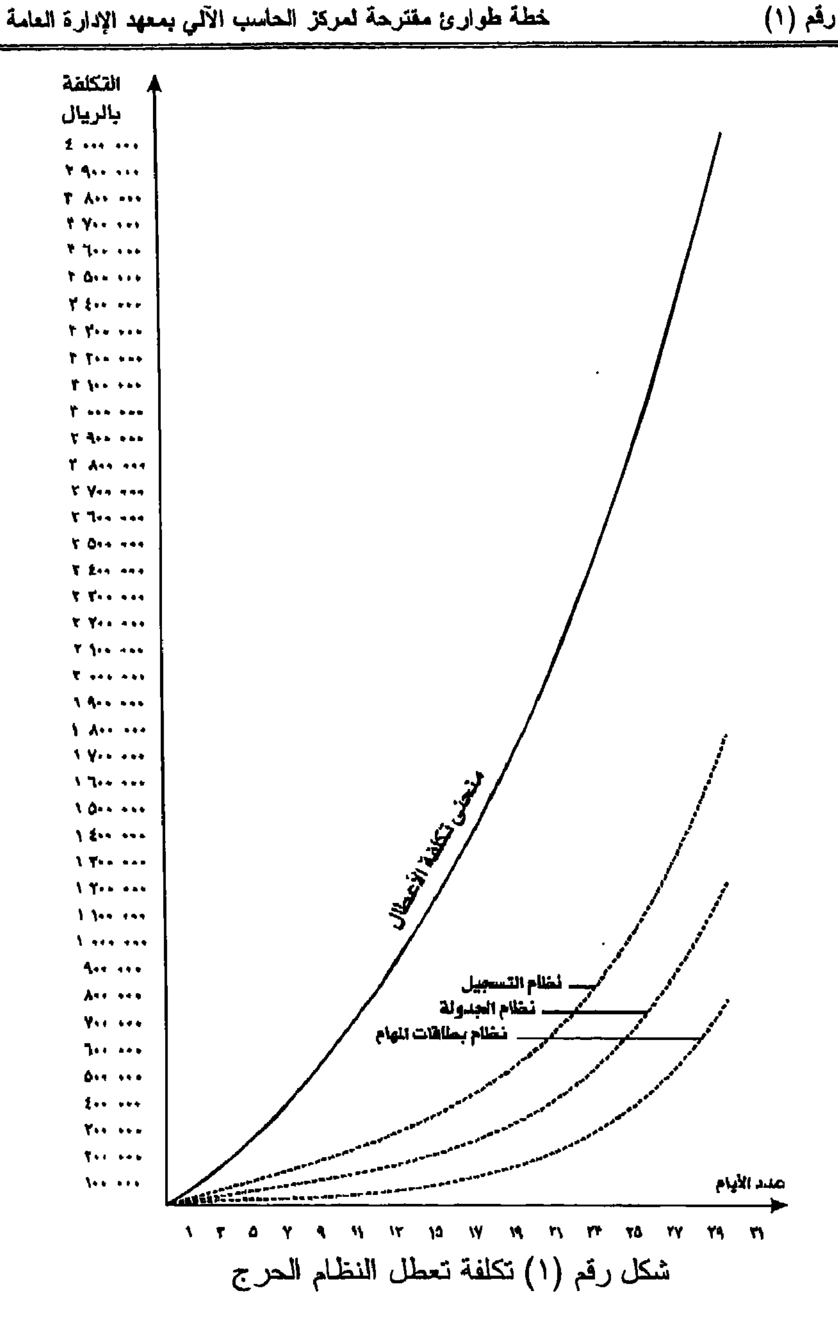
٨- **عدم كفاية ضوابط استخدام الطرفيات والنظام ككل:** وهذا واضح من خلال إمكانية العمل على الطرفيات مساء بدون وجود أي قيود، وكذلك وجود المفاتيح الخاصة بالمركز مع عمال غير موثوق بهم.

وبذلك ظهرت الحاجة إلى ضرورة تلافي هذه الأسباب قدر المستطاع ليتم التغلب على هذه الأخطار.

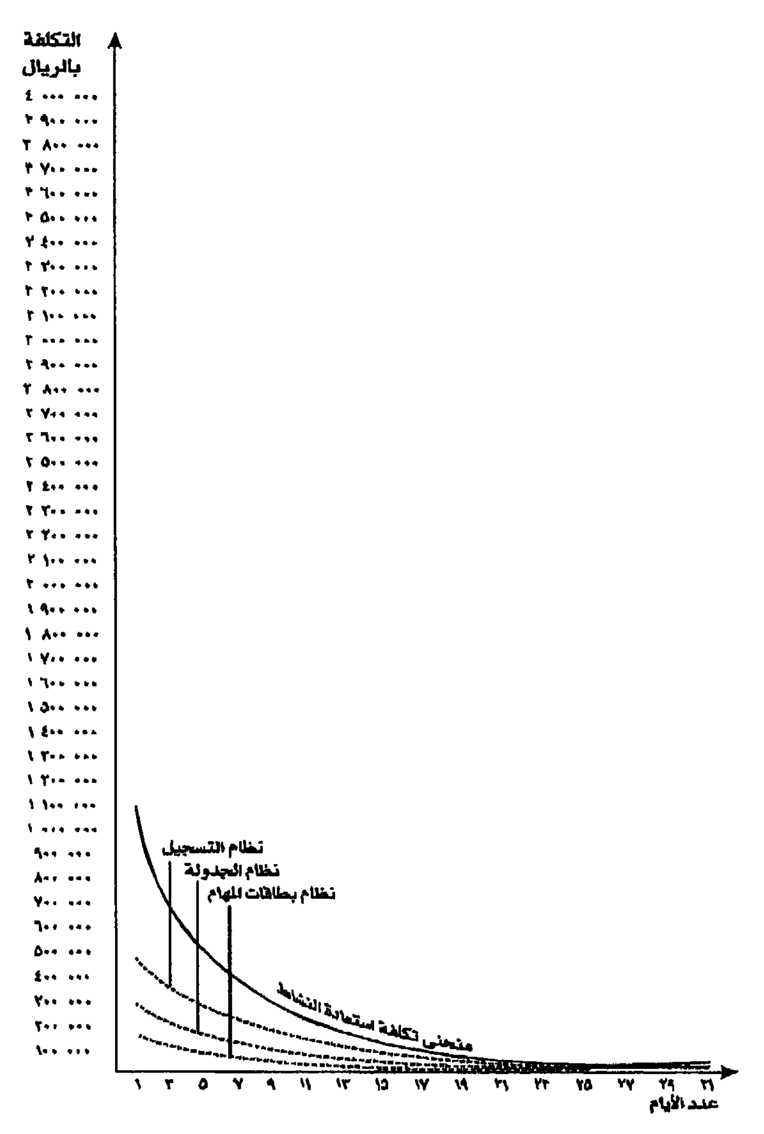
و ـ تحليل الأنظمة الحرجة بالمعهد:

الأخطار تهدد حياة الإنسان وممتلكاته وهي قد تحدث في أي لحظة بقدرة الله، ونتيجة لوقوعها تحدث فوضى وإرباك للعمل والعاملين مما قد يؤدي إلى نتائج غير طيبة، خاصة إذا كانت الجهة المعنية غير مستعدة لمواجهة مثل هذه المخاطر أو غير قادرة على احتوائها في ظل التغير المفاجئ الذي يحدث وينتج عنه اختلال التوازن للمنظمة.

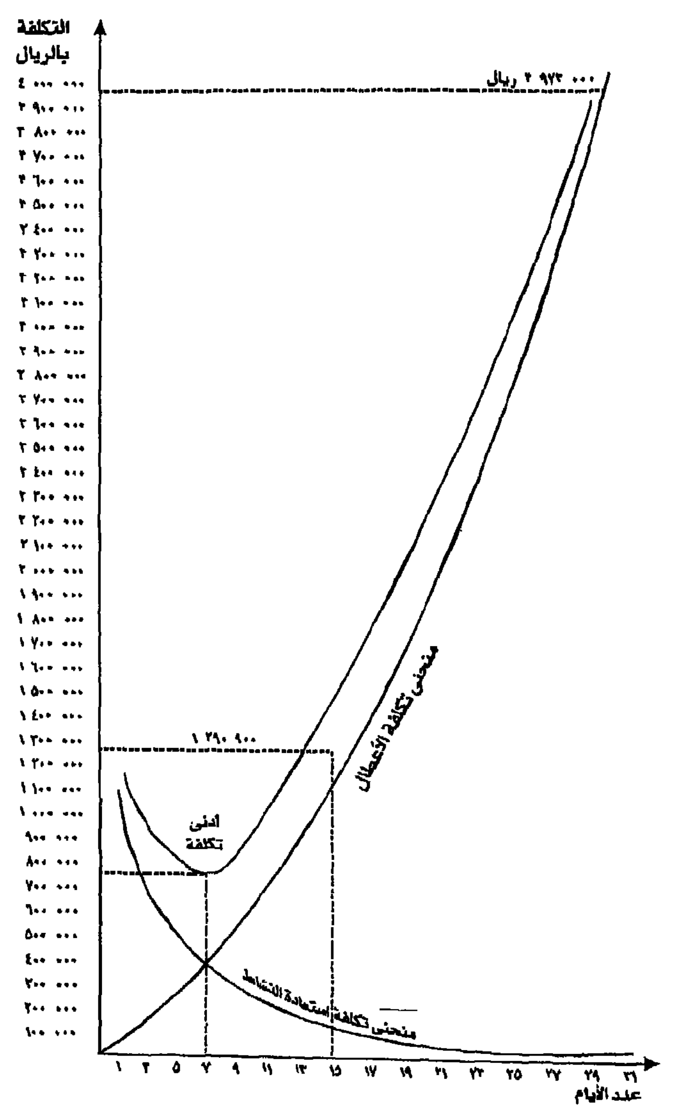
إن مرحلة إعادة التوازن إلى الوضع الطبيعي قبل حدوث الكارثة وتأمين الحد الأدنى الممكن من إعادة الحياة والنشاط للمنظمة يتم بإعادة تشغيل (الأنظمة الحرجة) التي لا يمكن أن يقوم المعهد بأداء دوره بدونها. ولذلك وبعد أن قمنا بتحديد ومعرفة الأنظمة الحرجة لمعهد الإدارة العامة باتباع طريقة علمية سليمة ودقيقة وعرفنا أن النظام الحرج للمعهد هو (نظام التسجيل بفروعه)، لذلك سنقوم بتحليله لوضع التخطيط السليم الذي يضمن استعادة المعهد لنشاطه الرئيسي ألا وهو التدريب والذي يمثل نظام التسجيل عصبه الحيوي، وذلك يتطلب التجهيز المسبق للموارد اللازمة لجعل عملية استعادة النشاط تتم في أقصر وقت وتحديد وتطبيق كافة الإجراءات والأنشطة والموارد اللازمة لتمكين المعهد من تقليل المخاطر إلى الحد الأدنى واستعادة نشاطه بعد حدوث التعطل المفاجئ لنظام الحاسب ولخدمات نظام التسجيل وفروعه بافتراض استمرار العطل لفترة قد تتجاوز سبعة أيام وهذه هي المدة التي تمثل عندها أدنى نقطة على منحنى "محصلة تكلفة العطل" كما يتضح من الشكل رقم (٣) "أدنى تكلفة لاستعادة النظام".



شكل رقم (١) تكلفة تعطل النظام الحرج



شكل رقم (٢) تكلفة استعادة النشاط



شكل رقم (٣) أدنى تكلفة لاستعادة النشاط

ز ـ اختيار البديل المناسب:

كما نعلم فإنه يوجد عدد من البدائل المتاحة لكي نستخدم إحداها كبديل لمركز الحاسب الآلي، واختيار هذا البديل يتم على أساس مدى الحاجة لاستعادة تشغيل النظام الحرج في أقل وقت ممكن وبأقل تكاليف ممكنة. وبناءًا على الدراسة التي أجريت واللقاءات التي تمت مع المسؤولين بمركز الحاسب الآلي اتضح أن أقصى مدة يمكن الاستغناء عن مركز الحاسب الآلي خلالها هي ٧ أيام في حالة حدوث كارثة، وأنه لابد من استعادة النشاط خلال ٧ أيام فقط. لذلك فإن أنسب بديل هو البديل "**نصف الفوري**". وهذا البديل هو الأنسب لمركز الحاسب الآلي بمعهد الإدارة العامة بالرياض في حالة حدوث كارثة لا سمح الله. والبديل نصف الفوري من الممكن أن يكون غرفة أخرى بالمعهد أو أن يكون مركز حاسب آلي بمؤسسة أخرى يستخدم كبديل لمعهد الإدارة والعكس صحيح أي بحيث يستخدم مركز المعهد كبديل لهذه المؤسسة في حالة حدوث الكارثة لديها، بشرط أن تكون الأنظمة والأجهزة المستخدمة في المؤسستين متطابقة. ولكن وجد أن هذا الحل يحتاج إلى تنسيق وإلى تكلفة تجهيزات إضافية لدى الطرفين، لذلك تم اختيار الحل الأول للبديل نصف الفوري وهو تخصيص صالة أو غرفة تستخدم كبديل لمركز الحاسب الآلي بحيث يمكن تجهيزها خلال ٧ أيام من وقت حدوث الكارثة.

وقد وقع الاختيار على القاعة رقم (٢٠) بالدور الأرضي بمبنى المعهد القديم لتكون مركزًا بديلاً. وهذه القاعة كانت من قبل غرفة لتشغيل أول جهاز حاسب استخدمه المعهد في عام ١٤٠٠هـ وهي بالتالي معدة من ناحية البنية التحتية الضرورية لتشغيل الحاسب. وسوف تخصص القاعة رقم (٢١) بالدور الأرضي بالمبنى القديم أيضًا لتنقل إليها الأصول الثمينة في حالة إخلاء المبنى.

(٤) إجراءات الطوارئ في مركز الحاسب

أ ـ الخطوة الأولى: إخلاء الموقع

وهو التحرك الأول في سلسلة إجراءات الطوارئ ويتوقف حجم الإخلاء على حجم وطبيعة الكارثة وذلك تبعًا للحالات التالية:

١) إخلاء عام لجميع العاملين بالمركز بأسرع ما يمكن.

٢) استثناء فريق الطوارئ من الإخلاء العام للإشراف على إخلاء العاملين وتنفيذ إجراءات الطوارئ الأساسية مثل: تشغيل أجهزة مكافحة الحريق وأجهزة الخدمات البديلة كالكهرباء والماء وإنقاذ الأصول الحساسة أو تأمينها.

٣) إخلاء غير فوري لكون الكارثة غير مفاجأة، فيجب على فريق الطوارئ العمل بسرعة ولكن بطريقة صحيحة فيتم إطلاق الإنذار وإيقاف العمل في المركز ونقل الأشياء ذات القيمة وبعض وسائط المعلومات إلى المكان الآمن وهو الغرفة رقم (٢١) بمبنى المعهد القديم.

ب ـ الخطوة الثانية: إبلاغ الجهات المختصة

يجب إبلاغ الجهات ذات العلاقة حسب التعليمات الموضوعة من واقع المرفق للخطة، وذلك للتدخل أو التوقف عن العمل وتكون بالترتيب التالي:

١) رئيس مركز الحاسب أو من يمثله في إحدى نوبات العمل.

٢) إدارة الدفاع المدني.

٣) مدير إدارة التشغيل والصيانة بالمعهد.

٤) مسئول أمن المعلومات بمركز الحاسب (والذي توصي الدراسة بتعيينه).

٥) باقي أفراد فريق الطوارئ والبدلاء للغائبين منهم، والتأكد من تجمعهم في نقطة تجمع محددة وهي الحديقة الكائنة بين المبنيين القديم والجديد للمعهد.

٦) مديرو الإدارات المستفيدة من المهددين بقطع الخدمة وفقًا للقائمة المرفقة.

٧) المسئولون عن تشغيل الموقع البديل وعن القاعتين رقم ٢٠ ، ٢١ بالدور الأرضي في مبنى المعهد القديم.

٨) شركة (آمدال Amdahl) المسئولة عن توريد وصيانة الأجهزة.

٩) شركة (آي بي إم .I.B.M) المسئولة عن البرمجيات ونظم التشغيل.

ج ـ الخطوة الثالثة: التقويم الأولى لآثار الكارثة

يؤدي تنفيذ هذه الخطة إلى اختيار الأسلوب الذي سيتم فيه استعادة النشاط ففي هذه المرحلة يجب على فريق الطوارئ أن يحدد التالي:

١) مدى الحاجة إلى موقع العمل البديل (القاعة رقم ٢٠ بالدور الأول بالمبنى القديم)، أو الاكتفاء بإصلاح ما تلف في الموقع الأصلي.

٢) تقدير الوقت المتوقع لاستعادة النشاط لكافة الأجهزة والنظم الحرجة خاصة نظام التسجيل.

ويتم ذلك بعمل تقويم أولي شامل لأثار الكارثة يهدف إلى تحديد الخسائر، والأصول التي تعطلت تمامًا عن العمل، والأصول التي يمكن إعادتها للعمل بسرعة، وموقف نظام التسجيل ومدى الضرر الذي حاق بملفاته.

د ـ الخطوة الرابعة: استعادة النشاط

بعد تحديد أسلوب استعادة النشاط حسب التقويم الأولي لآثار الكارثة يبدأ

إخطار المستفيدين في المعهد وخارجه بالمدة التي سوف يستغرقها ذلك، إما بأن يكون العمل في نفس مركز الحاسب بعد إصلاح وتأمين الأجهزة والبيانات والأفراد وما يلزمها من خدمات مختلفة أو بالمركز البديل. مع التأكد بأن المدة القصوى لعمل ذلك واستعادة نشاط النظام الحرج وهو نظام التسجيل هي سبعة أيام يتم العمل خلالها بالنظام اليدوي، ويجب الاستفادة من العقد المبرم مع شركة "آمدال" في هذا المجال فيتم الاتصال بهم لإصلاح الأجهزة التي لم يستطع موظفو المركز إصلاحها وتأمين قطع الغيار اللازمة وخلافه.

وفي حالة فقد الملفات أو البيانات فيتم اللجوء إلى النسخ الاحتياطية التي يجب أن تكون محفوظة بطريقة صحيحة في موقع بعيد عن المركز المتضرر (قاعة رقم ٢١ بالمبنى القديم)، وفي حالة فشل ذلك لسبب أو لآخر يتم اللجوء للطريقة اليدوية الموضوعة سلفًا. وبالنسبة للعاملين فتوجد قائمة بأسماء بديلة من خارج المركز في حالة فقدان الخبرات المتخصصة في المركز لا سمح الله، كما يمكن اللجوء إلى خبراء من شركة (IBM) وتنصح الدراسة بالتعاقد مع الشركة على ذلك. ويمكن اللجوء إلى الملحق الخاص المرفق بأسماء وعناوين الموظفين والبدلاء والمستفيدين والشركات.

نظرًا لكثافة الحركة والأعمال في هذه الخطوة فيجب تأمين تسهيلات عديدة لإنجاز تلك الأعمال بطريقة مرنة وسريعة. ومن بين تلك الخدمات، يجب حراسة المداخل والمخارج ومنع الغرباء من الدخول إلى الأماكن الحساسة وذلك بواسطة ضابط أمن المعلومات وأفراده المدربين على ذلك والذين يعرفون جميع العاملين بالمركز. كما يجب تأمين وسائل نقل الأجهزة إلى الموقع البديل ، ووسائط التخزين البديلة للبيانات، ولابد من تأمين وسائل الاتصالات والهواتف والشبكات ووسائل تبادل البيانات مع من يلزم من خارج المعهد، وإعادة التيار الكهربائي والمياه والمجاري، أو تشغيل وحدة الطاقة المتنقلة التي نوصي بضرورة توفيرها، ولابد

من إصلاح وتعويض الأثاث والأدوات المكتبية والأشرطة الممغنطة وغيرها ممـــا قد يكون تعرض للتلف.

هـ ــ الخطوة الخامسة: تشغيل الموقع البديل

(القاعة رقم ٢٠ بالدور الأول بالمبنى القديم).

في حالة تأكيد فريق تقويم آثار الكارثة لاستحالة تشغيل الموقـــع الأصلـــي فيجب اللجوء إلى هذه الخطوة. ولذلك ننصح بضرورة إجراء اختبـــارات تشـــغيل متكررة على فتراتٍ لا تزيد عن ستة أشهر وحل المشكلات التي قد تظهر.

في حالة تدمير البيانات والملفات في الكارثـــة يتـــم اللجـــوء إلـــى النســـخ الاحتياطية المحفوظة في موقع آمن بعيدًا عن مركز الحاسب (القاعة ٢١)، بعد ذلك يتم مباشرة إعادة تحميل البيانات من وسائط التخزين الاحتياطية بواسطة موظفـــي مركز الحاسب، وبعدها يتم إدخال التعديلات اللازمة علـــى رمـــوز المســـتخدمين وكلمات المرور وباقي جداول نظام التشغيل لتعكس البيئة الجديدة، وبعد ذلـــك يتـــم تحميل التطبيقات الحرجة فقط وهي نظام التسجيل والأنظمة الثلاثة المرافقة.

يختبر التشغيل في البيئة الجديدة ويتم حل أي مشكلة، بعدهـــا يتـــم تحديـــث الملفات لتغطية فترة التوقف، ولذلك نوصي بضرورة أن تكون النسخ الاحتياطيـــة للبيانات حديثة، ووجود قاعدة بيانات يوفر ميزة ممتازة في هـــذه الحالـــة لوجـــود البيانات في وعاء واحد وبيئة واحدة.

وتتاح الخدمة للمستفيدين بالتدريج بدءًا بنظام "التسجيل" ثم نظام "الجدولة" ثـــم نظام "بطاقات المهام" وتراقب العملية جيدًا ويوضع حل لأي مشكلة قد تظهر.

و ــ الخطوة السادسة: إعادة الخدمة للمستفيدين

حيث إن الموقع البديل يعتبر موقعًا مؤقتًا فلابد أن يعود التشغيل إلى الموقـــع الأصلي بأسرع وقت ولابد من تقدير الوقت اللازم لاستعادة كل ذلك كشراء أجـــهزة

بديلة وتركيب نظم التشغيل والبرمجيات. بعد أن يكون مركز الحاسب المتضرر جاهزًا يتم استخدامه بثقة وعدم تسرع، بعكس تشغيل الموقع البديل، وكذلك يتم تركيب واختبار التطبيقات "غير الحرجة" بالمركز الأصلي أولاً وحل المشاكل. وأخيرًا يتم نقل التطبيقات الحرجة واختبارها. لأن طول مدة التعطل يتسبب في تراكم كميات من البيانات المطلوب إدخالها ومعالجتها فيلزم تأمين معالجة تلك البيانات وحفظها وتجهيزها للمستفيدين بعد تدقيقها وسوف يتطلب ذلك عددًا أكبر من الموظفين ويقترح تكليف الموظفين بالعمل خارج الدوام لإتمام ذلك، ولا نتوقع أن يتطلب الأمر مساعدة خارجية.

(٥) مهام الفرق المشاركة

يتكون فرق الطوارئ المناط به مواجهة أي حالة أو كارثة تؤدي إلى تعطل أو توقف أنظمة الحاسب في مركز الحاسب الآلي من مجموعات عمل مدربة تدريبًا مكثفًا لأداء مهامها حسب خطة الطوارئ الموضوعة. ويضم هذا الفريق في عضويته ممثلين عن كافة الإدارات المستفيدة بالمعهد وجميع إدارات مركز الحاسب الآلي بأكملها. كما تمثل فيه الإدارة العليا ومركز الحاسب الآلي على أعلى مستوى ممكن.

ويتكون الفريق من المجموعات التالية:

أ ــ الإدارة:

تتكون من نائب مدير عام المعهد للبحوث والمعلومات رئيسًا للفريق ، ومدير إدارة الدعم الفني بمركز الحاسب الآلي نائبًا للرئيس، وتتمثل المهام في التالي:

١) التأكد من وجود خطة طوارئ فعالة وإنها تختبر وتصان دائمًا.
٢) إدارة عملية استعادة النشاط وتنسيق عمل الفرق المشاركة.
٣) إعلام الإدارة بالتطورات وتقديم تقارير دورية عن الوضع.

ب ـ الإخلاء والأمن:

ويتكون هذا الفريق من ضابط أمن المعلومات بالمركز وعدد من الموظفين المدربين على أعمال الأمن والإسعافات الأولية ولهم معرفة بجميع العاملين بمركز الحاسب الآلي، ومهامهم كالتالي:

١) توجيه النداء المناسب لحظة وقوع الكارثة لإخلاء مركز الحاسب.
٢) تنفيذ إجراءات الطوارئ الأولية.
٣) نقل الأصول الحساسة والأوراق المهمة إلى مكان آمن.
٤) تنفيذ الإجراءات الأمنية لتأمين الأصول والمداخل والمخارج ومنع دخول الغرباء.

ج ـ التقويم الأولى للكارثة:

يعتبر عمل هذا الفريق من أهم الخطوات التي تحدد مدى الحاجة إلى القاعة رقم ٢٠ بالدور الأرضي بالمبنى القديم أو إصلاح ما تلف في مركز الحاسب الآلي بالمعهد ومهامه كالتالي:

١) تقويم أولي شامل لآثار الكارثة.
٢) فحص سريع للأصول المختلفة بمركز الحاسب من أجهزة وبرمجيات وأفراد ومعلومات بهدف تحديد الخسائر والأصول التي تعطلت تمامًا والأصول التي يمكن إعادتها للعمل.
٣) تحديد موقف النظم الحرجة الثلاثة ومدى الضرر الذي حاق بها.
٤) تقدير الوقت المتوقع لاستعادة النشاط للأجهزة والنظم الحرجة.

د ــ المساندة والتسهيلات:

يتركز عمل الفريق في مساندة الفرق الأخرى بإمدادها بالفنيين المتواجدين في المعهد في أمور مثل: خدمات الكهرباء والماء والمجاري والهاتف وتوفير عمال لنقل الأجهزة والأثاث ووسائط التخزين للبيانات. ومهامهم كالتالي:

١) نقل الأجهزة ووسائط تخزين البيانات والأفراد.
٢) الاتصال بالجهات المختصة حسب الترتيب من واقع الملحق الخاص بذلك.
٣) تأمين أجهزة الاتصالات وخدمة الهاتف والشبكات ووسائل تبادل البيانات.
٤) إعادة التيار الكهربائي والمياه والمجاري في مركز الحاسب الآلي المتضرر أو في القاعة رقم ٢٠ بالدور الأرضي بالمبنى القديم كصالة بديلة للمركز عند اللزوم.
٥) توفير الأثاث والأدوات المكتبية والأقراص والأشرطة الممغنطة وغيرها.

هـ ــ مركز الحاسب الآلي:

يتكون هذا الفريق من ممثلين لجميع إدارات أو أقسام مركز الحاسب الآلي بإشراف كبير المبرمجين ويجب التنسيق المسبق للاستعانة بخبرات خارجية في حالة فقد بعض المتخصصين نتيجة الكارثة وذلك بالاستفادة من العقد المبرم مع شركة IBM ، ويعتبر مطورو النظم والمشغلون ومبرمجو النظم ومسئولو قاعدة البيانات من أهم عناصر الفريق. والمهام تتمثل في الآتي:

١) استعادة النشاط لنظام التدريب الحرج ممثلا بنظام التسجيل وغيره.
٢) التأكد من وجود نسخ احتياطية حديثة بشكل دائم وتأمينها بعيدًا.
٣) تشغيل الأجهزة بعد استكمالها سواء في مركز الحاسب الآلي المتضرر جزئيًا أو في القاعة رقم ٢٠ بالدور الأول بالمبنى القديم أو البديل.
٤) تحميل نظام التشغيل والبرمجيات المرافقة.

٥) إعادة تحميل البيانات من وسائط التخزين الاحتياطية.
٦) إدخال التعديلات على رموز المستخدمين وكلمات المرور وباقي جداول النظام لتعكس البيئة الجديدة.
٧) تحميل التطبيقات الحرجة كنظام التسجيل والتدريب على البرمجة فقط.
٨) اختبار التشغيل في البيئة الجديدة وحل المشكلات المعترضة.
٩) بعد ذلك يتم إعادة الخدمة المعتادة للمستفيدين بالتدريج.

(٦) اختبار خطة الطوارئ ومراقبتها وتعديلها

نظرًا لاحتمال وجود نقاط ضعف في خطة الطوارئ يصعب اكتشافها قبل تطبيق الخطة، فإن اختبار الخطة خير وسيلة للاطمئنان إلى أنها ستعمل بكفاءة عند وقوع الكارثة (لا قدر الله).

وقد تبدو عملية الاختبار مكلفة لما تتطلبه من وقت ومال إضافة إلى الأفراد وإمكانات الحاسب الآلي ، إلا أنه بمقارنة تكاليف إجراء الاختبار مع ما يسببه وقوع الكارثة من خسائر في حالة عدم كفاءة الخطة، فإنه يتبين عدم صحة هذه النظرة.

أ ـ أهداف الاختبار:

١) التأكد من أن درجة التعرض للخطر في الحدود المقبولة.
٢) التأكد من أن خطة استعادة النشاط تعمل بصورة سليمة.
٣) اختبار فاعلية الخطة واكتشاف مواطن الضعف فيها وتحديد المجالات التي تتطلب تعديل التدابير الموضوعة أو تلك التي تحتاج إلى إضافة تدابير جديدة.

٤) تعويد الموظفين على التآلف مع إجراءات الطوارئ وتعزيز شعورهم بالمسئولية، والتأكد من استيعابهم للخطة وقدرتهم على تنفيذها بدقة تلافيًا للفوضى وتصادم القرارات والتصرفات العشوائية.
٥) التدريب فالاختبار في حد ذاته هو نوع من تدريب الموظفين على تنفيذ الخطة.

ب ـ أسلوب اختبار الخطة:

١) **اختبار الخطة على الورق:** تتم مراجعة تقسيم الفرق وتحديد مهامها وتوزيع الصلاحيات والتأكد أنه لا يوجد تضارب أو تداخل بينها.
٢) **اختبار إجراءات الطوارئ الأساسية:** يتم هذا الاختبار بشكل عشوائي مفاجئ للتأكد من اتباع إجراءات الطوارئ الأساسية مثل إخلاء الموقع بشكل عام.
٣) **اختبار الخطة الفعلي:** يعتبر تطبيق الخطة هو أفضل اختبار لها، ويتم هذا الاختبار بصفة دورية منتظمة. وأبسط طرق الاختبار هي إعلان توقف الحاسب عن العمل ثم مراقبة الخطوات التي يتم اتباعها لإعادته إلى العمل. وهذا الأسلوب بالإضافة إلى بساطته فهو أقل الأساليب كلفة وأقدرها على اكتشاف الثغرات لتلافيها فيما بعد.

ج ـ العوامل التي يجب أخذها في الاعتبار عند اختبار الخطة:

١) ألا يقل معدل إجراء الاختبارات عن مرتين في السنة.
٢) أن تشمل الاختبارات أكبر عدد ممكن من الموظفين (ولو بالتناوب).
٣) تسجيل النتائج ونقاط القوة والضعف ووضعها في ملاحق الخطة تمهيدًا لاستخدامها أثناء مراجعة الخطة وصيانتها.
٤) أهمية الاستعانة بالمختصين في مجال أمن المعلومات والطوارئ من خارج المركز لمراقبة الاختبارات التي تجري على الخطة وكتابة ملاحظاتهم عليها وكشف أوجه القصور فيها.

٥) البدء باختبار أجزاء الخطة كل على حدة ثم يتلو ذلك اختبار متكامل للخطة بأكملها للتأكد من تناغم هذه الأجزاء مع بعضها، مع مراعاة أنه لا يوجد فشل في هذه الاختبارات فإذا لم تنجح مرحلة من المراحل فهذا يعد نجاحًا في حد ذاته لأنه كشف ثغرة ما في الخطة تتطلب المعالجة وهذا أحد أهداف اختبار الخطة.

٦) أهمية إحاطة الإدارة العليا بنتائج الاختبار.

د ـ أسلوب مراقبة الخطة وإدخال التعديلات عليها:

تتم مراقبة الخطة بواسطة فريق الطوارئ للتأكد من إدخال التعديلات المطلوبة عليها وضمان استجابتها للمتغيرات، وقد تقرر مراجعة الخطة كل ستة أشهر على الأكثر وإدخال التعديلات اللازمة عليها. مع الإشارة إلى أنه قد يتطلب الأمر إجراء المراجعة وإدخال التعديلات قبل مضي هذه المدة وذلك في حالة:

١) القيام بعملية اختبار للخطة يتم من خلالها تدوين نقاط الضعف والقوة في الخطة، إضافة إلى ملاحظات المتخصصين في أمن المعلومات الذين تمت الاستعانة بهم لمراقبة التجربة.

٢) حدوث تغيير في العمل الرئيسي للمعهد وبالتالي تغير الأنظمة الحرجة التي تم بناء الخطة على أساسها أو حدوث تغيير في بيئة الحاسب أو الأجهزة أو البرمجيات أو نظم التشغيل أو النظم التطبيقية التي تمت الإشارة إليها في الخطة.

وبعد الانتهاء من صيانة الخطة وإدخال التعديلات عليها تعرض على الإدارة لاعتمادها في شكلها الجديد.

(٧) أسلوب توعية وتدريب الموظفين على تنفيذ الخطة

يشمل أسلوب توعية وتدريب الموظفين على تنفيذ الخطة ما يلي:

١) التحاق الأفراد الأساسيين في تنفيذ الخطة بدورة أمن الحاسبات التي ينظمها المعهد لمدة ثلاثة أسابيع.

٢) إقامة دورة لمدة يومين للتدريب على تنفيذ الخطة يلتحق بها جميع الموظفين في مركز الحاسب الآلي وتتكرر هذه الدورة بصفة دورية بحيث ينضم لها كل من يلتحق للعمل بالمركز حديثًا إضافة إلى الأفراد المناط بهم المشاركة في تنفيذ الخطة.

٣) تقديم محاضرة عامة لموظفي المعهد مدتها ساعتان ضمن "لقاء الأربعاء" الذي ينظمه المعهد ويتم خلال هذه المحاضرة شرح الخطة وأهدافها، والرد على استفسارات موظفي المعهد.

٤) عرض فيلم يوضح عملية الإخلاء والأخطاء التي ترتكب خلالها.

٥) طباعة كتيب للتوعية بقضايا أمن الحاسبات مع التركيز على الأوضاع الخاصة بالمركز.

٦) الاستفادة من اختبار الخطة في تدريب الموظفين لمنحهم الثقة بالنفس وهو ما يحتاجون إليه عند حدوث الكارثة الحقيقية (لا قدر الله).

(٨) ملاحق الخطة

أ ـ قائمة المشاركين في تنفيذ الخطة (*)

م	الاسم	الوظيفة	الهاتف	البديل	الوظيفة	الهاتف

(*) تم حذف أسماء الموظفين والبدلاء لأغراض أمن الخطة.

ب ـ مكونات النظام البديل

م	البيان	العدد	التكلفة بالريال
	أولا: الأجهزة HARDWARE		
١	CPU IBM 390	١	٥٠٠,٠٠٠
٢	LINE PRINTERS	١	٢٠,٠٠٠
٣	TERMINALS	٢٠	١٠٠,٠٠٠
٤	DASD	٤	١٢٠,٠٠٠
٥	UNIT TAPE DRIVES	٢	١٠٠,٠٠٠
٦	COMMUNICAION CONTROLLERS	٤	١٠٠,٠٠٠
٧	MULIPLEXERS	٤	٧,٠٠٠
٨	UPS	١	١٠٠,٠٠٠
	ثانيا البرمجيات: SOFTWARE		مجانا لاستخدامها بنفس الترخيص
١	MVS/XA		
٢	ACF/VTAM 3.3.0		
٣	PASCAL COMPILER		
٤	COBOL COMPILER		
٥	CICS/MVS 2.1.2		
٦	DB2 2.2.0		
٧	JES2 2.2.3		
٨	TSO/E 2.1.0		
	ثالثا التطبيقات: APPLICATIONS		
	أشرطة النسخ الاحتياطية الخاصة بالتطبيقات وتتضمن: - مكتبة برامج التطبيقات. - ملفات التطبيقات (البيانات).		يمكن إهمال القيمة

ج ـ الميزانية المخصصة

البيان	التكلفة بالريال
أولاً: التجهيزات الضرورية لغرفة الحاسب تمديد الكابلات خطي هاتف طفايات حريق (UPS)	٢٠,٠٠٠ ١٠٠,٠٠٠
ثانيًا: الأجهزة الضرورية للمركز البديل	١,٠٤٧,٠٠٠
ثالثًا: البرمجيات	مجانًا لاستخدامها بنفس الترخيص
رابعًا: تكاليف إعداد الخطة وصيانتها	١٥٦,٠٠٠
خامسًا: تكلفة التدريب	١٠٠,٠٠٠
سادسًا: تكلفة اختبار الخطة	١٠,٠٠٠
	١,٤٣٣,٠٠٠

د ـ قائمة بالإمكانات المتاحة

م	البيان	الاستخدامات
١	القاعة رقم ٢٠ في الدور الأرضي بمبنى المعهد القديم.	يمكن استخدامها كمركز بديل مؤقت.
٢	القاعة رقم ٢١ في الدور الأرضي بمبنى المعهد القديم.	يمكن استخدامها كقاعة تدريب لمتدربي المعهد ولحفظ الأشرطة.
٣	١٠ أتوبيسات ١٠ سيارات	نقل البيانات. نقل الموظفين.
٤	عمال النظافة (٩٠)	المساعدة في عمليات الإخلاء. المساعدة في عمليات الإطفاء.
٥	عيادة طبية	تقديم الإسعافات الأولية للمصابين.
٦	المطعم	تقديم الوجبات في المعهد بدلاً من مغادرة الموظفين إلى خارج المعهد لتناول الوجبات.

هـ ــ قائمة بالجهات المستفيدة من داخل المعهد (٣/١)

الجهة (*)	الهاتف
الإدارة العامة	
معالي المدير العام	١١٨١
سعادة نائب المدير العام للتدريب	١١٠٢
سعادة نائب المدير العام للبحوث والمعلومات	١١٠٠
اللجنة العليا للإصلاح الإداري	١١١٥
إدارة الاستشارات	١١٠٤
المراقب المالي	١١٤٤
إدارة العلاقات العامة والإعلام	١١٦٦
التطوير الإداري	١١٣٤
إدارة التخطيط	١١٩٠
إدارة البحوث	١١٢٦
إدارة تصميم وتطوير البرامج	١٦٨٦
إدارة تقييم البرامج	١٦٢٨
إدارة البرامج العليا	١٤٥٥
إدارة البرامج الخاصة	١١٢٤
إدارة البرامج المالية والاقتصادية	١٤٥٧
إدارة البرامج الإدارية	١٤٥٠
إدارة برامج الاتصال التنظيمي والعلاقات	١٤٥٣
إدارة البرامج الهندسية	١٣٣١
إدارة برامج الحاسب الآلي	١٢٣٥
إدارة برامج الإدارة المكتبية	١٦٣٠
إدارة برامج القطاع الأهلي	١٦٦٣
مركز اللغة الإنجليزية	١٦٠٠
إدارة علاقات المتدربين	١٨١٠٠
إدارة شئون المتدربين	١٥٨٧
إدارة القبول والتسجيل	١٥٨٢

(*) ربما اختلفت بعض مسميات الإدارات أو أرقام هواتفها منذ إعداد الخطة المقترحة.

هـ ـ قائمة بالجهات المستفيدة من داخل المعهد (٢/٣)

الجهة (*)	الهاتف
مركز تقنيات التدريب	١٤٨٠
مركز الحاسب الآلي: مدير مركز الحاسب الآلي	١٥٦٣
سكرتير الإدارة	١٥٣٧
مدير العمليات والتشغيل	١٥٧٥
مدير التطبيقات وتطوير الأنظمة	١٥١٢
مدير خدمات المستفيدين	١٢٣١
خدمات المستفيدين	١١٧٧
مركز المصغرات الفيلمية	١٥٦٤
الإدارة العامة للمكتبات	١٤٧٠
إدارة الوثائق الحكومية السعودية	١٤٦٢
إدارة تنمية المجموعات	١٤٧٢
إدارة تنظيم المجموعات	١٤٧١
إدارة خدمات المعلومات	١٤٠١
إدارة تقنية المعلومات	١٤٣٣
إدارة الطباعة والنشر	١٥٨١
الشئون الإدارية والمالية	١١٦٩
الشئون المالية	١١٤٣
شئون الموظفين	١١٥٥
المشتريات	١١٦١
مركز الاتصالات الإدارية	١٥٧٧
المستودعات	١٥٥٩
التشغيل والصيانة	١١٧٨
الأمن والسلامة	١٥٦٠

(*) ربما اختلفت بعض مسميات الإدارات أو أرقام هواتفها منذ إعداد الخطة المقترحة.

هـ ـ قائمة بالجهات المستفيدة من داخل المعهد (٣/٣)

الجهة (*)	الهاتف
منسقو القطاعات: إدارة المواد	١٣٥٥
الإحصاء	١٣٧١
الإدارة الصحية	١٤٢٤
الإدارة العامة	١٣١٥
الإدارة المكتبية	١٦٥٩
الإدارة الهندسية والمشروعات	١٣١٣
الاقتصاد والميزانية	١٣٨٠
التعليمية والتدريبية	١٣٠٥
الحاسب الآلي	١٢٨٠
السلوك الإداري	١٤٢١
العلاقات العامة والإعلام	١٣٨٤
القانون	١٣٠٤
المحاسبة	١٣٤٠
شئون المكتبات	١٣٣٩
شئون الموظفين	١٣٨٥
القطاع الأهلي	١٦٣٨
منسق الندوات	١١٨٤
منسق الحلقات التطبيقية	١١٨٦

(*) ربما اختلفت بعض مسميات الإدارات أو أرقام هواتفها منذ إعداد الخطة المقترحة.

و ـ قائمة بالجهات المستفيدة من خارج المعهد (٣/١)

الجهة (*)	الهاتف
وزارة الأشغال العامة والإسكان	٤٠٢٣٣٣٣
وزارة الإعلام	٤٠٦٨٨٨٨
وزارة البترول والثروة المعدنية	٤٧٨٧٧٧٧
وزارة البريق والبريد والهاتف	٤٦٣٤٤٤٤
وزارة التجارة	٤٠١٢٢٢٢
وزارة التخطيط	٤٠١٣٣٣٣
وزارة التعليم العالي	٤٤١٥٥٥٥
وزارة الحج	٤٠٢٦٠٢١
وزارة الخارجية	٤٠٥٥٠٠٠
وزارة الداخلية	٤٠١١١١١
وزارة الدفاع والطيران	٤٧٨٩٠٠٠
وزارة الزراعة والمياه	٤٠١٢٧٧٧
وزارة الشئون الإسلامية والأوقاف	٤٧٣٠٤٠١
وزارة الشئون البلدية والقروية	٤٥٦٩٩٩٩
وزارة الصحة	٤٠١٢٢٢٠
وزارة الصناعة والكهرباء	٤٧٧٦٦٦٦
وزارة العدل	٤٠٥٧٧٧٧
وزارة العمل والشئون الاجتماعية	٤٧٧٨٨٨٨
وزارة المالية الاقتصاد الوطني	٤٠٥٠٠٠٠
وزارة المعارف	٤٠٤٦٦٦
وزارة المواصلات	٤٠٤٣٠٠٠
اتصال منطقة الرياض	٤٥٤١٠١٠
إدارة البحوث والإفتاء والدعوة والإرشاد	٤٥٩٥٥٥٥
الإدارة العامة لمكافحة المخدرات	٤٧٩١٠٤٠
البنك الزراعي العربي السعودي	٤٠٢٢٣٥٩
الدار السعودية للخدمات والاستشارات	٤٤٨٤٥٣٣

(*) ربما اختلفت بعض مسميات الجهات أو أرقام هواتفها منذ إعداد الخطة المقترحة.

و ــ قائمة بالجهات المستفيدة من خارج المعهد (٢/٣)

الجهة (*)	الهاتف
الديوان العام للخدمة المدنية	٤٠٢٦٦٦٦
الرئاسة العامة لتعليم البنات	٤٠٥٦١١١
الرئاسة العامة لرعاية الشباب	٤٠١٤٥٧٦
الصندوق السعودي للتنمية	٤٦٤٠٢٩٢
الغرفة التجارية الصناعية بالرياض	٤٠٤٠٠٤٤
القوات البحرية الملكية السعودية	٤٧٧٦٧٧٧
القوات الجوية الملكية السعودية	٤٧٦٩٧٧٧
المؤسسة العامة لتحلية المياه المالحة	٤٦٣١١١١
المؤسسة العامة لصوامع الغلال	٤٦٤٣٥٠٠
المؤسسة العامة للتأمينات الاجتماعية	٤٧٧٧٧٣٥
المؤسسة العامة للتعليم الفني والتدريب	٤٠٥٢٧٧٠
المؤسسة العامة للكهرباء	٤٧٧٦٦٦٦
المؤسسة العامة للموانئ	٤٠٥٠٠٠٥
المديرية العامة لحرس الحدود	٤٠٢٠٢٢٢
المديرية العامة للأحوال المدنية	٤٦٢٦٦٦٦
المديرية العامة للأمن العام	٤٤١٥٠٥٠
المديرية العامة للجوازات	٤٧٧١١٠٠
المديرية العامة للدفاع المدني	٤٧٨٩٩٩٩
المؤسسة العامة لخطوط السكك الحديدية	٤٤٨٠٠٠٠
الهيئة العربية السعودية للمواصفات والمقاييس	٤٥٢٠٠٠٠
الهيئة العليا لتطوير مدينة الرياض	٤٨٨٣٣٣١
الهيئة الملكية للجبيل وينبع	٤٧٩٤٤٤٥
إمارة منطقة الرياض	٤١١٤٤٤٤
أمانة مدينة الرياض	٤١١٢٢٢٢
بنك التسليف السعودي	٤٠٢٩١٢٨

(*) ربما اختلفت بعض مسميات الإدارات أو أرقام هواتفها منذ إعداد الخطة المقترحة.

و ـ قائمة بالجهات المستفيدة من خارج المعهد (٣/٣)

الجهة (*)	الهاتف
جامعة الإمام محمد بن سعود الإسلامية	٢٥٨٠٠٠٠
جامعة الملك سعود	٤٦٧٠٠٠٠
جوازات الرياض	٤٠٢٠٠٠٠
دارة الملك عبد العزيز	٤٤١٢٣١٦
ديوان المراقبة العامة	٤٠٥٦٧٧٠
ديوان المظالم	٤٠٢١٧٢٤
رئاسة الحرس الوطني	٤٩١٢٢٢٢
رئاسة مجلس الوزراء	٤٨٨٢٥٥٥
صندوق التنمية الصناعية السعودي	٤٧٧٤٠٠٢
مؤسسة النقد العربي السعودي	٤٦٣٢٠٠٠
مجلس التعاون لدول الخليج العربية	٤٨٢٧٧٧٧
مجلس الشورى	٤٨٢١٦٦٦
مدينة الملك عبد العزيز للعلوم والتقنية	٤٨٨٣٥٥٥
مرور الرياض	٤٤١٥٢٢٢
مصلحة الإحصاءات العامة	٤٠٥٩٦٣٨
مصلحة الجمارك	٤٠١٣٣٣٤
مصلحة الزكاة والدخل	٤٠٤٤٣٧٥
مصلحة معاشات التقاعد	٤٠٢٢٨١٨
مكتب التوظيف بالمنطقة الوسطى	٤٦٣٠١١١
هيئة الأمر بالمعروف والنهي عن المنكر	٤٣٥٠٠٠٠
هيئة التحقيق والإدعاء العام	٤٦٢٨٢٦٦
هيئة الرقابة والتحقيق	٤٠٥٢٨٠١
وكالة الأنباء السعودية	٤٦٢٣٣٣٣

(*) ربما اختلفت بعض مسميات الإدارات أو أرقام هواتفها منذ إعداد الخطة المقترحة.



المؤلف في سطور

المهندس/ حسن أحمد طاهر داود

- من مواليد جمهورية مصر العربية في ١٧/٢/١٩٤٦م.

المؤهل العلمي:

- ماجستير هندسة الحاسب من جامعة جرينوبل بفرنسا يونيو ١٩٧٨م.
- بكالوريوس هندسة الاتصالات من جامعة عين شمس بالقاهرة يونيو ١٩٦٩م.

الوظيفة الحالية:

- عضو هيئة التدريب بمعهد الإدارة العامة ـ الرياض.

الأنشطة العلمية

- مجالات الاهتمام: أمن المعلومات، قواعد البيانات، شبكات المعلومات والإنترنت.
- مؤلف كتاب "جرائم نظم المعلومات" أكاديمية نايف العربية للعلوم الأمنية ٢٠٠٠م ، وعدد من البحوث والمقالات المنشورة.
- مقرر ندوة "شبكات المعلومات وقواعد البيانات الموزعة" الرياض ١٩٩٨م.
- عضو مجلس إدارة جمعية الحاسبات السعودية ورئيس فرع الرياض بها.
- منح عام ١٩٩٦ الجائزة العالمية:

(The World Lifetime Achievement Award)
من مؤسسة (American Biographical Institute) الأمريكية تقديرًا لجهوده في خدمة مجتمع الحاسب الآلي بالمملكة.

- تم اختياره في عام ١٩٩٨م من قبل مؤسسة:

(International Biographical Center) ومقرها بريطانيا ضمن المتميزين إبداعيًا خلال القرن عن نشاطاته في مجال الحاسب الآلي.

تصميم وإخراج وطباعة
الإدارة العامة للطباعة والنشر بمعهد الإدارة العامة - ١٤٢١هـ



هذا الكتاب

يطرق هذا الكتاب موضوعًا هامًا وحيويًا يمس حياة الأفراد ، كل الأفراد ، كما يمس مصائر الدول ، كل الدول ، فهو يتحدث عن أمن المعلومات وأمن مراكز الحاسب الآلي ، وعن جرائم الحاسب ومنها الفيروسات وأساليب مكافحتها ويدعو المؤسسات التشريعية في الدول العربية لأن تسن قوانينها الخاصة بمكافحة جرائم الحاسب ، ويدعو لإنشاء إدارة لأمن المعلومات في وزارات الداخلية العربية .

يتحدث الكتاب كذلك عن مواجهة الكوارث واستمرارية العمل وتحليل الأخطار المحتملة التي تواجه مراكز الحاسب ، ويقدم منهجية جديدة في تحليل المخاطر ويدعو خبراء أمن المعلومات لاتباعها ، كما يتعرض لموضوع على جانب كبير من الأهمية وهو «خطة الطوارئ المعلوماتية» ، فيتحدث عنها بالتفصيل ويقدم في ملحقه خطة طوارئ فعلية يمكن أن تحتذى .

يتعرض الكتاب لتشفير البيانات وأنواع التشفير مثل التشفير باستخدام المفتاح العلني ، والتشفير المودع ، وتشفير المكالمات الهاتفية . كما يتحدث عن نظم أمن البيانات المتاحة في الأسواق وكيفية المفاضلة بينها ، وعن تصنيف مراكز الحاسب الآلي وفقًا لاتباعها لمعايير أمن المعلومات .

يتطرق الكتاب لأمن التطبيقات ، وأمن قواعد البيانات ، والمشاكل الأمنية في بيئة «العميل/الخادم» ، كما يتعرض لأمن شبكات نقل المعلومات ، ومصادر تهديد البيانات خلال مرورها بالشبكة ، وأمن شبكات (إنترانت) وهو الهاجس الذي يشغل بال الكثير من الشركات التي تستخدم تقنيات الإنترنت في شبكاتها المحلية ، ويهتم الكتاب بأمن الإنترنت ، فيتحدث عن الأخطار الأمنية المحيطة بها ، وشبكة «إنترنت ٢» الجديدة ، وعن تقنيات حماية المعلومات فيها مثل جدران الحماية ومدى فاعليتها .

لعل القارئ بعد قراءة هذا الكتاب أن ينظر إلى أمن المعلومات نظرة مختلفة وأكثر حرصًا ، فأمن المعلومات قد يكون الفاصل بين النصر والهزيمة في الحـ الفيصل بين البقاء والفناء لدول أو أفراد أو مؤسسات أو شركات .

ردمك : ٨-٦

تصميم وإخراج وطباعة
الإدارة العامة للطباعة والنشر بمعهد الإدارة العامة - ١٤٢١هـ